HAL
archives-ouvertes.fr

Points de torsion des courbes elliptiques et équations diophantiennes

Nicolas Billerey

▶ **To cite this version:**

Nicolas Billerey. Points de torsion des courbes elliptiques et équations diophantiennes. Mathématiques [math]. Université Pierre et Marie Curie - Paris VI, 2009. Français. <tel-00446928>

HAL Id: tel-00446928

https://tel.archives-ouvertes.fr/tel-00446928

Submitted on 13 Jan 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Université Pierre et Marie Curie – Paris 6

École Doctorale Paris Centre

Thèse de doctorat

Discipline : Mathématiques

présentée par

Nicolas Billerey

Points de torsion des courbes elliptiques et équations diophantiennes

---

dirigée par Alain Kraus

Soutenue le 19 novembre 2009 devant le jury composé de :

M. Daniel Bertrand	Université Pierre et Marie Curie	Examinateur
M. John Boxall	Université de Caen Basse-Normandie	Examinateur
M. Yann Bugeaud	Université de Strasbourg	Examinateur
M. Alain Kraus	Université Pierre et Marie Curie	directeur
M. Joseph Oesterlé	Université Pierre et Marie Curie	Examinateur
M. Pierre Parent	Université Bordeaux 1	Rapporteur

Institut de Mathématiques de Jussieu
175, rue du chevaleret
75 013 Paris

École doctorale Paris centre Case 188
4 place Jussieu
75 252 Paris cedex 05

Remerciements

Je voudrais tout d'abord adresser mes remerciements à mon directeur de thèse Alain Kraus. Au cours des innombrables heures de travail qu'il m'a consacrées, j'ai pu apprécier sa droiture, son professionnalisme et sa générosité. Il a su m'encadrer de très près tout en me laissant la liberté d'aborder par moi-même d'autres questions. Son soutien constant m'a permis de ne jamais me décourager même lorsque mes perspectives mathématiques ou professionnelles y auraient incité.

Je suis particulièrement honoré que Michael Bennett et Pierre Parent aient accepté de rapporter mon travail. Je connais et j'admire leurs travaux mathématiques et j'ai eu la chance, lors de ma dernière année de thèse, de rencontrer Pierre Parent à Bordeaux.

J'apprécie la confiance que John Boxall m'a témoignée en acceptant de participer à mon jury et en m'invitant à venir faire un exposé à Caen. Je connais Yann Bugeaud depuis mes années strasbourgeoises et l'ai parfois sollicité depuis pour des questions auxquelles il a toujours répondu avec célérité et précision. Ses qualités de mathématicien et d'orateur sont un exemple. Je suis très heureux que l'un et l'autre fassent partie de mon jury.

Durant mes années de thèse, j'ai côtoyé presque quotidiennement Daniel Bertrand et Joseph Oesterlé. C'est un plaisir et un honneur qu'ils participent à mon jury.

Je voudrais également remercier tous les membres de l'équipe de théorie des nombres de l'IMJ au sein de laquelle j'ai pris plaisir à travailler. Plus particulièrement, Dominique Bernardi pour son aide sur le logiciel `pari`, Pierre Charollois pour l'intérêt qu'il a porté au dernier chapitre de ma thèse et Marc Hindry dont j'ai souvent sollicité les compétences mathématiques et footballistiques !

Si j'ai pu mener à bien ce travail, c'est aussi grâce au soutien de l'équipe administrative. Je pense en particulier à Marcelline Prosper-Cojande pour sa gentillesse et son dévouement et Gilles Godefroy pour l'intérêt qu'il a toujours porté aux doctorants en tant que directeur de l'Institut.

Cette thèse n'aurait jamais vu le jour sans les efforts de nombreux mathématiciens. Parmi eux, Henri Darmon et Jean-Pierre Serre ont eu la gentillesse de relire certains passages de mon travail. Leurs commentaires sont aussi précis que précieux.

Durant quatre années, j'ai suivi le cours de Don Zagier au Collège de France. J'y ai appris autant sur les mathématiques que sur la façon d'en faire. Il a eu la gentillesse de lire une version préliminaire du dernier chapitre de ma thèse. Ses nombreuses remarques ont largement contribué à en améliorer le fond comme la forme.

Je connaissais Luis Dieulefait par ses travaux lorsque j'ai eu la chance de pouvoir collaborer avec lui. J'ai été frappé par son humilité et j'espère que nous aurons à nouveau l'occasion de travailler ensemble. Il m'a de plus offert la possibilité d'exposer pour la première fois mes travaux dans un séminaire. Depuis j'ai eu l'occasion de le faire dans d'autres instituts : merci à Éric Gaudron, Pieter Moree, Marusia Rebolledo, Gaël Rémond et David Vauclair pour les invitations.

Grâce au soutien financier de l'IMJ, de l'équipe de théorie des nombres et du réseau européen GTEM, j'ai pu effectuer de nombreux séjours et participer à plusieurs conférences qui ont été autant d'enrichissements mathématiques et personnels. Merci également au HIM de Bonn pour l'accueil chaleureux des mois de mars et avril 2009.

Merci à tous les doctorants qui ont accepté de gré ou de force de participer au Séminaire des Étudiants en Théorie des Nombres lorsque je l'organisais.

Un immense merci à tous mes amis doctorants de l'institut (avec une pensée spéciale pour ceux du 7B04) et d'ailleurs dont la liste est si longue que je ne pourrais pas les citer tous sans en oublier et avec qui j'ai partagé repas quasi-quotidiens, séminaires (secrets ou non), cafés, thés, parties de foot, pique-niques, soirées, vacances... et qui ne manqueront pas de venir m'aider à déménager !

Merci à mes fidèles soutiens strasbourgeois, Étienne et Olivier, et visiteurs à chevaleret, Gilles et Manu.

Merci à ma (belle-)famille pour leur soutien constant et l'intérêt qu'ils portent à ce que je fais.

À Perrine enfin, et à notre Étienne qui fêtera son premier mois le jour de la soutenance de son papa, mais qui sait déjà que un et un font trois !

Introduction

Cette thèse se compose de deux parties principales contenant chacune deux chapitres. Dans la première partie, on étudie quelques équations diophantiennes à l'aide de la « méthode modulaire ». La seconde partie est consacrée à l'arithmétique des courbes elliptiques et notamment de leurs points d'ordre fini.

Première partie

Elle comporte deux chapitres portant chacun sur un cas particulier de la conjecture suivante.

Conjecture 0.1 *Soient $F \in \mathbb{Z}[X,Y]$ une forme homogène séparable de degré ≥ 3 et d un entier ≥ 1. Il existe une constante $C_{d,F} > 0$ ne dépendant que de d et F telle que si p est un nombre premier $> C_{d,F}$ et (a,b,c) un triplet d'entiers non nuls premiers entre eux vérifiant l'égalité*

$$F(a,b) = dc^p,$$

alors on a $c = \pm 1$.

Dans toute cette partie, on dit qu'un triplet (a,b,c) d'entiers est une solution de l'équation

$$F(x,y) = dz^p \tag{1}$$

si $F(a,b) = dc^p$, qu'elle est *propre* si a, b et c sont premiers entre eux dans leur ensemble et qu'elle est *non triviale* si $abc \neq 0$.

Dans le premier chapitre, on s'intéresse au cas où

$$F(X,Y) = X^5 + Y^5.$$

Dans le second chapitre, on considère plus spécifiquement le cas où F est une forme cubique.

Chapitre 1

Étant donné un entier $d \geq 1$ libre de puissances cinquièmes et un nombre premier p, on note $S_p(d)$ l'ensemble des solutions propres et non triviales de l'équation (1) dans le cas où

$$F(X,Y) = X^5 + Y^5.$$

À tout élément $(a, b, c) \in S_p(d)$, Darmon associe la courbe elliptique $E(a, b)$ suivante :

$$y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x.$$

En utilisant les propriétés de modularité de la courbe $E(a, b)$ démontrées par Wiles ([Wil95]) et Breuil, Conrad, Diamond et Taylor ([BCDT01]), on obtient, pour plusieurs valeurs de l'entier d, des résultats sur les ensembles $S_p(d)$ lorsque p varie.

Ce chapitre a été publié au *Bulletin of the Australian Mathematical Society* en 2007 ([Bil07]). Par la suite, Luis Dieulefait et moi-même avons amélioré ces résultats dans une publication commune à paraître à *Mathematics of Computation* ([BD08]).

Chapitre 2

La conjecture 0.1 est une conséquence de la conjecture *abc* de Masser et Oesterlé. Dans le cas où F est de degré 3, on construit[1] un polynôme $G(X, Y, Z)$ de degré 3 en la variable Z tel que

$$\mathrm{disc}_Z G(X, Y, Z) = \mathrm{disc}(f) \cdot F(X, Y)^2,$$

où disc_Z désigne le discriminant par rapport à la variable Z et $\mathrm{disc}(f)$ le discriminant du polynôme $f(X) = F(X, 1)$. Cette construction généralise celle de Frey pour la forme cubique

$$F(X, Y) = XY(X + Y)$$

associée à l'équation de Fermat, ainsi que celle de Darmon pour la forme

$$F(X, Y) = X^3 + Y^3.$$

Étant donnée une solution propre et non triviale (a, b, c) de l'équation (1), cette construction fournit alors en toute généralité une courbe elliptique d'équation

$$y^2 = G(a, b, x)$$

qui a les « bonnes » propriétés de ramification. Cela nous permet, toujours dans le cas des formes de degré 3, de réduire la conjecture 0.1 à une conséquence d'une conjecture de Frey et Mazur sur les modules galoisiens des points d'ordre premier des courbes elliptiques. À titre d'application, on détermine ensuite, pour plusieurs valeurs de l'entier d, l'ensemble des solutions propres et non triviales de l'équation (1) dans le cas où

$$F(X, Y) = X^3 + X^2Y + XY^2 + Y^3.$$

Les résultats de ce chapitre ont fait l'objet d'une publication [Bil08a] au *Journal of Number Theory* en mai 2008.

[1] Je remercie Don Zagier de m'avoir signalé cette formulation du résultat.

Seconde partie

Elle traite de l'arithmétique des courbes elliptiques et se compose de deux chapitres. Dans le premier, on s'intéresse au défaut de semi-stabilité des courbes elliptiques à réduction additive avec potentiellement bonne réduction définies sur les extensions finies de $\mathbf{Q}_2$. Dans la seconde partie on étudie certaines propriétés galoisiennes des points d'ordre fini des courbes elliptiques définies sur un corps de nombres.

Chapitre 3

Soient K une extension finie de $\mathbf{Q}_2$ contenue dans une clôture algébrique fixée $\overline{\mathbf{Q}_2}$ de $\mathbf{Q}_2$ et E une courbe elliptique définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier. Il existe alors une plus petite extension L de la clôture non ramifiée K_{nr} de K dans $\overline{\mathbf{Q}_2}$ où E acquiert bonne réduction. Le groupe $\Phi = \mathrm{Gal}(L/K_{nr})$ est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe à un groupe quaternionien, soit d'ordre 24 et isomorphe à $\mathrm{SL}_2(\mathbf{F}_3)$. Sa détermination précise n'a été menée que dans deux cas : par A. Kraus pour $K = \mathbf{Q}_2$ ([Kra90]) et par É. Cali pour toutes les extensions finies $K/\mathbf{Q}_2$ non ramifiées ([Cal04]).

Dans ce chapitre, on commence par établir en fonction de la valuation de j modulo 12 plusieurs résultats généraux sur le groupe Φ, valables pour toute extension finie $K/\mathbf{Q}_2$. Dans tous les cas restants, la connaissance de la valuation de j modulo 12 ne suffit pas à déterminer l'ordre du groupe Φ.

D'autre part, dans le cas des extensions quadratiques ramifiées de $\mathbf{Q}_2$, on détermine explicitement le groupe Φ en fonction des coefficients d'une équation de Weierstrass de E. Combiné avec les travaux de Cali et Kraus, ce dernier résultat achève le calcul du groupe Φ pour toutes les extensions de $\mathbf{Q}_2$ de degré ≤ 2.

Ce chapitre a été soumis en juin 2008 à la revue *Dissertationes Mathematicae*.

Chapitre 4

Soient K un corps de nombres contenu dans la clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ dans $\mathbf{C}$ et E une courbe elliptique définie sur K. On dit qu'un nombre premier p est exceptionnel pour le couple (E, K) si la représentation

$$\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \longrightarrow \mathrm{Aut}(E[p])$$

donnant l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ sur le sous-groupe $E[p]$ des points de p-torsion de E est réductible. On s'intéresse dans ce chapitre à la détermination explicite de l'ensemble des nombres premiers exceptionnels pour le couple (E, K). Il est bien connu que si E n'a pas de multiplications complexes sur $\overline{\mathbf{Q}}$, cet ensemble est fini. En utilisant des arguments de théorie du corps de classes, on obtient un critère portant sur la réduction de E en chaque place finie de K permettant d'aborder la question suivante.

Question 1. Le corps K et la courbe E étant donnés, peut-on décider en toute généralité si l'ensemble des nombres premiers exceptionnels est fini et si tel est le cas comment le déterminer explicitement ?

Comme conséquence du résultat principal que l'on obtient à ce sujet, on démontre notamment que pour toute courbe elliptique définie sur un corps de degré impair sur $\mathbf{Q}$, l'ensemble des nombres premiers exceptionnels est fini et qu'il est inclus dans l'ensemble des diviseurs premiers d'une collection explicite d'entiers (dépendant de (E, K)).

On s'intéresse également dans ce chapitre à la question suivante.

Question 2. Étant donnés un corps de nombres K et un ensemble infini $\mathcal{E}$ de courbes elliptiques définies sur K, peut-on trouver une constante uniforme $\alpha(\mathcal{E}, K)$ telle que pour toute courbe elliptique E appartenant à $\mathcal{E}$, la représentation ρ_p soit irréductible dès que $p > \alpha(\mathcal{E}, K)$?

La réponse à cette question n'est, bien entendu, pas toujours positive. À l'aide des résultats obtenus au chapitre 3 et d'arguments de la théorie du corps de classes, on obtient plusieurs énoncés en direction de la question 2 pour des ensembles $\mathcal{E}$ de courbes elliptiques ayant mauvaise réduction additive en une place finie de K et un « défaut de semi-stabilité » particulier.

On illustre les résultats obtenus en déterminant explicitement l'ensemble des nombres premiers exceptionnels de plusieurs couples (E, K), notamment si K est une extension quadratique de $\mathbf{Q}$.

Table des matières

Première partie

Équations diophantiennes

Chapitre 1

Équations de Fermat de type $(5, 5, p)$

Ce chapitre reproduit sans modification l'article [Bil07] paru au Bulletin of the Australian Mathematical Society. *Signalons que ces résultats ont par la suite été généralisés par Luis V. Dieulefait et moi-même et sont à paraître dans une publication commune ([BD08]).*

Introduction

Soient d un entier naturel sans puissances cinquièmes et p un nombre premier ≥ 7. On s'intéresse dans cet article à l'équation diophantienne suivante :

$$x^5 + y^5 = dz^p. \tag{1.1}$$

Suivant la terminologie de H. Darmon et A. Granville ([DG95]), on dira qu'un triplet d'entiers $(a, b, c) \in \mathbf{Z}^3$ est une solution de l'équation (1.1) si l'on a $a^5 + b^5 = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Notons $S_p(d)$ l'ensemble des solutions propres et non triviales de l'équation (1.1). On se propose dans cet article de démontrer quelques résultats concernant l'ensemble $S_p(d)$. Une conséquence de la conjecture abc est la suivante :

Conjecture 1.1 *Supposons que d ne soit pas la somme de deux puissances cinquièmes d'entiers relatifs non nuls. Alors, il existe une constante $c(d)$, qui ne dépend que de d, telle que si l'on a $p > c(d)$, alors l'équation (1.1) n'admet aucune solution propre et non triviale.*

Les travaux de G. Frey, K. A. Ribet, J.-P. Serre et A. Wiles sur les représentations modulaires, permettent parfois d'aborder ce type de problèmes (cf. [Fre86], [Rib90], [Ser87] et [Wil95]). La méthode maintenant fréquemment utilisée à ce sujet est souvent appelée la méthode modulaire. Elle exploite les propriétés modulaires de certaines courbes elliptiques ainsi que les propriétés galoisiennes de leurs points de p-torsion. Plus précisément, à une hypothétique solution de l'équation (1.1), on associe ici une courbe elliptique sur $\mathbf{Q}$, dont la construction

est dûe à H. Darmon ([Dar97]), dite *courbe de Frey* ou *courbe de Hellegouarch-Frey* et dont la représentation galoisienne dans ses points de p-torsion est liée à l'existence d'une forme modulaire de poids et de niveau précis, qui « essentiellement » ne dépendent pas de la solution considérée. On est alors confronté au problème de démontrer que l'existence d'une telle forme modulaire conduit à une contradiction. Une étude de la ramification du corps des points de p-torsion de la courbe de Frey permet parfois d'y parvenir.

Signalons qu'un résultat figurant dans [Kra02] entraîne que, p étant donné, l'ensemble des entiers d sans puissances cinquièmes et sans diviseurs premiers congrus à 1 modulo 5, pour lesquels $S_p(d)$ soit non vide, est fini. Dans cet article, nous mettons en œuvre la méthode modulaire et certaines de ses variantes pour l'étude de l'équation (1.1). Elle permet de montrer que $S_p(d)$ est vide pour $p \geq 7$, ou seulement pour une infinité de p, dans certains cas où d est de la forme $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ avec $0 \leq \alpha, \beta, \gamma \leq 4$.

On énonce par ailleurs un critère, analogue à celui obtenu par A. Kraus concernant l'équation $x^3 + y^3 = z^p$ (cf. [Kra98]), permettant souvent de montrer que $S_p(3)$ est vide pour un nombre premier p fixé. On démontre qu'il s'applique également aux petites valeurs de p (notamment $p = 7$). On le vérifie numériquement, à l'aide d'un programme `pari/gp` pour tous les nombres premiers p compris entre 7 et 10^6.

1.1 Énoncés des résultats

Soit p un nombre premier ≥ 7. Les résultats décrits ici concernent les entiers d de la forme

$$d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma, \quad \text{avec} \quad 0 \leq \alpha, \beta, \gamma \leq 4.$$

Dans le cas particulier où $d = 1$, en utilisant la méthode modulaire classique, on obtient l'énoncé suivant :

Théorème 1.2 *Soit (a, b, c) un élément de $S_p(1)$. Alors c est impair. Autrement dit, la puissance p-ième d'un entier pair non nul ne peut s'écrire comme la somme de deux puissances cinquièmes d'entiers premiers entre eux.*

Pour quinze valeurs de d sur les cent vingt-cinq envisagées ci-dessus, par la même méthode que celle utilisée dans le théorème 1.2, on obtient une réponse complète quant à la description de $S_p(d)$:

Théorème 1.3 *Supposons que d soit de la forme*

$$d = 2^\alpha \cdot 5^\gamma \quad \textit{avec } \alpha \in \{2, 3, 4\} \quad \textit{et} \quad 0 \leq \gamma \leq 4.$$

Alors, $S_p(d)$ est vide.

Pour certaines valeurs de d, nous obtenons une réponse partielle en démontrant que $S_p(d)$ est vide seulement pour un ensemble de nombres premiers p de densité > 0. En utilisant la méthode symplectique, décrite dans [HK02], on obtient à ce sujet l'énoncé suivant :

Théorème 1.4 *Posons $d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$ et supposons que l'on soit dans l'un des cas ci-dessous :*

1. $(\alpha, \beta, \gamma) \in \{(3,1,\geq 1),(3,4,\geq 1),(4,2,\geq 1)\}$ *et* $p \equiv 5$ *ou* $7 \pmod{12}$;
2. $(\alpha, \beta, \gamma) \in \{(3,2,\geq 1),(4,1,\geq 1),(4,4,\geq 1)\}$ *et* $p \equiv 7, 11, 13$ *ou* $17 \pmod{24}$;
3. $(\alpha, \beta, \gamma) \in \{(3,1,0),(3,4,0),(4,2,0),(4,3,0)\}$ *et* $p \equiv 5$ *ou* $19 \pmod{24}$;
4. $(\alpha, \beta, \gamma) = (4,3,\geq 1)$ *et* $p \equiv 3$ *ou* $5 \pmod{8}$.

Alors, $S_p(d)$ *est vide.*

Énonçons maintenant les résultats obtenus concernant le cas où $d = 3$. Pour tout nombre premier $p \geq 7$, on démontre un critère qui permet souvent de prouver que $S_p(3)$ est vide. Considérons pour cela un nombre premier q congru à 1 modulo p. Posons $q = np + 1$. Le groupe $\mu_n(\mathbf{F}_q)$ des racines n-ièmes de l'unité de $\mathbf{F}_q$ est d'ordre n. On définit deux sous-ensembles $A(n,q)$ et $B(n,q)$ de $\mu_n(\mathbf{F}_q)$ de la façon suivante.

1. Soit $\widetilde{A}(n,q)$ le sous-ensemble de $\mu_n(\mathbf{F}_q)$ formé des éléments ζ pour lesquels :

$$405 + 62500\zeta \text{ est un carré dans } \mathbf{F}_q.$$

   À un tel élément ζ, on associe le plus petit entier $\delta_{1,\zeta} \geq 0$ tel que

$$\delta_{1,\zeta}^2 \pmod{q} = 405 + 62500\zeta.$$

   On définit $A(n,q)$ comme étant le sous-ensemble de $\widetilde{A}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

$$-225 + 10\delta_{1,\zeta} \quad \text{et} \quad -225 - 10\delta_{1,\zeta}$$

   est un carré modulo q. À tout élément $\zeta \in A(n,q)$, on associe alors la cubique sur $\mathbf{F}_q$ suivante :

$$F_{1,\zeta} : y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{1.2}$$

   Son discriminant vaut $6480\zeta^2 = 2^4 \cdot 3^4 \cdot 5\zeta^2$, qui est non nul car on a $q \geq 7$. Par suite, $F_{1,\zeta}$ est une courbe elliptique sur $\mathbf{F}_q$. On note $n_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbf{F}_q$ de $F_{1,\zeta}$ et l'on pose

$$a_q(\zeta) = q + 1 - n_{1,q}(\zeta). \tag{1.3}$$

2. Soit $\widetilde{B}(n,q)$ le sous-ensemble de $\mu_n(\mathbf{F}_q)$ formé des éléments ζ pour lesquels :

$$405 + 20\zeta \text{ est un carré dans } \mathbf{F}_q.$$

   À un tel élément ζ, on associe le plus petit entier $\delta_{2,\zeta} \geq 0$ tel que

$$\delta_{2,\zeta}^2 \pmod{q} = 405 + 20\zeta.$$

   On définit $B(n,q)$ comme étant le sous-ensemble de $\widetilde{B}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

$$-225 + 10\delta_{2,\zeta} \quad \text{et} \quad -225 - 10\delta_{2,\zeta}$$

est un carré modulo q. À tout élément $\zeta \in B(n, q)$, on associe alors la cubique sur $\mathbf{F}_q$ suivante :

$$F_{2,\zeta} : y^2 = x^3 + \delta_{2,\zeta} x^2 + 5\zeta x. \tag{1.4}$$

Son discriminant $2^4 \cdot 3^4 \cdot 5^3 \zeta^2$ est non nul car on a $q \geq 7$. Par suite, $F_{2,\zeta}$ définit une courbe elliptique sur $\mathbf{F}_q$. On note $n_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbf{F}_q$ de $F_{2,\zeta}$ et l'on pose

$$b_q(\zeta) = q + 1 - n_{2,q}(\zeta). \tag{1.5}$$

Les notations étant celles utilisées dans les tables de [Cre97] (à ceci près que les lettres minuscules ont été remplacées ici par des lettres majuscules), on considère les trois ensembles de courbes elliptiques suivants :

$$\begin{aligned} \mathcal{E}_1 &= \{150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{J1}\}; \\ \mathcal{E}_2 &= \{150\text{A1}, 600\text{C1}, 1200\text{N1}\}. \end{aligned}$$

Si F est l'une des courbes des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ et si ℓ est un nombre premier ≥ 7, alors F a bonne réduction en ℓ. On pose

$$a_\ell(F) = \ell + 1 - |\widetilde{F}(\mathbf{F}_\ell)|,$$

où $|\widetilde{F}(\mathbf{F}_\ell)|$ est le nombre de points rationnels de la courbe $\widetilde{F}$ sur $\mathbf{F}_\ell$ déduite de F par réduction modulo ℓ.

Le critère que l'on obtient est le suivant :

Théorème 1.5 *Soit p un nombre premier ≥ 7. Supposons que les deux conditions suivantes soient satisfaites :*

1. *pour toute courbe elliptique F appartenant à $\mathcal{E}_1$, il existe un entier $n \geq 2$ tel que :*
   (a) *l'entier $q = np + 1$ est premier.*
   (b) *On a $a_q(F)^2 \not\equiv 4 \pmod{p}$.*
   (c) *Pour tout ζ dans $A(n, q)$, on a*
   $$a_q(\zeta)^2 \not\equiv a_q(F)^2 \pmod{p}.$$
2. *Pour toute courbe elliptique F appartenant à $\mathcal{E}_2$, il existe un entier $n \geq 2$ tel que :*
   (a) *l'entier $q = np + 1$ est premier.*
   (b) *On a $a_q(F)^2 \not\equiv 4 \pmod{p}$.*
   (c) *Pour tout ζ dans $B(n, q)$, on a*
   $$b_q(\zeta)^2 \not\equiv a_q(F)^2 \pmod{p}.$$

Alors, $S_p(3)$ est vide.

En utilisant ce critère et un résultat de L. Dirichlet concernant le cas où $p = 5$ ([Dir28]), on obtient l'énoncé suivant :

Proposition 1.6 *Si l'on a $5 \leq p \leq 10^6$, alors $S_p(3)$ est vide.*

Le critère du théorème 1.5 s'applique pour des valeurs de p considérablement plus grandes que 10^6. Ainsi $S_p(3)$ est vide lorsque $p = 15485863$ qui est le millionième nombre premier : on vérifie en effet que $n = 10$ satisfait aux conditions du théorème 1.5 (pour toute courbe F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$). De même, $S_p(3)$ est vide pour $p = 1000000007$. Il suffit de prendre $n = 44$.

On donne en Appendice un tableau de valeurs d'entiers n satisfaisant aux conditions du théorème 1.5 pour les nombres premiers compris entre 11 et 150, ainsi que quelques explications heuristiques sur l'efficacité de ce critère pour les « grands » nombres premiers.

1.2 La courbe elliptique E

On considère un élément (a, b, c) de $S_p(d)$. À un tel triplet on associe l'équation de Weierstrass E définie sur $\mathbf{Q}$:

$$y^2 = x^3 - 5(a^2+b^2)x^2 + 5\left(\frac{a^5+b^5}{a+b}\right)x. \tag{1.6}$$

Ses invariants standard (c_4, c_6, Δ) sont les suivants (cf. [Tat75]) :

$$\begin{cases} c_4 &= 2^4 \cdot 5\big(5(a^2+b^2)^2 - 3\frac{a^5+b^5}{a+b}\big) = 2^4 \cdot 5(2a^4+3ba^3+7a^2b^2+3ab^3+2b^4), \\ c_6 &= 2^5 \cdot 5^2(a^2+b^2)\big(2 \cdot 5(a^2+b^2)^2 - 3^2\frac{a^5+b^5}{a+b}\big) \\ &= 2^5 \cdot 5^2(a^6+9a^5b+12a^4b^2+18a^3b^3+12a^2b^4+9ab^5+b^6), \\ \Delta &= 2^4 \cdot 5^3(a+b)^2(a^5+b^5)^2. \end{cases}$$

Puisque (a, b, c) appartient à $S_p(d)$, E est une courbe elliptique définie sur $\mathbf{Q}$.

Notations.

1. On pose
$$r = \prod_{\ell \mid cd, \ell \neq 2,5} \ell,$$
où ℓ parcourt l'ensemble des diviseurs premiers de cd autres que 2 et 5.
2. Si ℓ est un nombre premier, on note v_ℓ la valuation ℓ-adique de $\mathbf{Q}$.
3. On pose
$$\phi(a, b) = \frac{a^5+b^5}{a+b} = a^4 - a^3b + a^2b^2 - ab^3 + b^4. \tag{1.7}$$
4. On note Δ_m le discriminant minimal de E.

Remarques préliminaires.

1. Les entiers a, b et c sont premiers entre eux deux à deux : cela résulte du fait que a, b et c sont premiers entre eux dans leur ensemble et que d est sans puissances cinquièmes.
2. Supposons d impair. Si a ou b est pair (mais pas les deux), alors c est impair. Si a et b sont impairs, alors c est pair.
3. Si d est pair, alors ab est impair.

4. Compte tenu des deux remarques précédentes, on peut supposer, ce que l'on fera dans toute la suite, que l'on est dans l'un des cas suivants :
   (a) d est impair et ac est pair : si c est impair, alors ab est pair et l'on suppose que c'est a qui est pair.
   (b) d est pair et ab impair.

Proposition 1.7 *L'équation (1.6) est minimale en dehors de 2. Elle est minimale en 2, auquel cas on a $\Delta_m = \Delta$, sauf dans les trois cas suivants :*

1. *les entiers d et a sont impairs (et c est pair) ;*
2. *les entiers d et c sont pairs ;*
3. *l'entier c est impair et l'on a $v_2(d) = 2$, 3 ou 4.*

Dans chacun de ces trois cas, on a alors :

$$\Delta_m = \frac{\Delta}{2^{12}}.$$

Soit N_E le conducteur de E.

Proposition 1.8 *Supposons d impair. On a :*

1. *$N_E = 2^4 \cdot 5^2 r$ si $v_2(a) = 1$;*
2. *$N_E = 2^3 \cdot 5^2 r$ si $v_2(a) \geq 2$;*
3. *$N_E = 2 \cdot 5^2 r$ si a est impair.*

Proposition 1.9 *Supposons d pair.*

1. *Si c est* pair, *on a $N_E = 2 \cdot 5^2 r$.*
2. *Si c est* impair, *alors :*
   (a) si $v_2(d) = 2$, on a $N_E = 5^2 r$;
   (b) si $v_2(d) = 3$ ou 4, on a $N_E = 2 \cdot 5^2 r$;
   (c) si $v_2(d) = 1$, on a $N_E = 2^4 \cdot 5^2 r$.

Les démonstrations de ces propositions font l'objet des paragraphes 1.2.1 à 1.2.5.

1.2.1 Lemmes préliminaires

Les trois lemmes suivants interviennent dans la suite à plusieurs reprises.

Lemme 1.10 *Soit ℓ un nombre premier divisant $a + b$. On a alors*

$$\phi(a, b) \equiv 5a^2b^2 \pmod{\ell^2}. \tag{1.8}$$

Démonstration. Si ℓ un nombre premier divisant $a + b$, on a

$$a^2 + b^2 \equiv -2ab \pmod{\ell^2}.$$

Or

$$\phi(a, b) = (a^2 + b^2)^2 - ab(a^2 + b^2 + ab), \tag{1.9}$$

d'où

$$\phi(a, b) \equiv 5a^2b^2 \pmod{\ell^2}$$

et le lemme 1.10

Lemme 1.11 *Les entiers $a+b$ et $\phi(a,b)$ sont premiers entre eux en dehors de 5. De plus, si 5 divise $a+b$, alors $v_5(\phi(a,b))=1$ et $v_5(a+b)=v_5(d)+pv_5(c)-1$.*

Démonstration. Soit ℓ un nombre premier divisant $a+b$ et $\phi(a,b)$. Si $\ell \neq 5$, on a $5a^2b^2 \not\equiv 0 \pmod{\ell}$ car ℓ ne divise pas ab. Donc ℓ ne divise pas $\phi(a,b)$ (lemme 1.10). Si $\ell = 5$, la congruence (1.8) ci-dessus implique $v_5(\phi(a,b))=1$. L'égalité $(a+b)\phi(a,b)=dc^p$ entraîne alors le lemme.

Lemme 1.12 *Soit ℓ un nombre premier non congru à 1 modulo 5 et divisant a^5+b^5. Alors, ℓ divise $a+b$.*

Démonstration. Puisque ℓ divise a^5+b^5, ℓ ne divise pas ab. Soit b' l'inverse de $-b$ modulo ℓ. On a $a^5 \equiv (-b)^5 \pmod{\ell}$, d'où $(ab')^5 \equiv 1 \pmod{\ell}$. Par suite, l'ordre de ab' dans le groupe multiplicatif $\mathbf{F}_\ell^*$ est 1 ou 5. La congruence $ab' \equiv 1 \pmod{\ell}$ conduit à $a+b \equiv 0 \pmod{\ell}$. Si ℓ ne divise pas $a+b$, on en déduit donc que l'ordre de ab' dans $\mathbf{F}_\ell^*$ est 5 puis $\ell \equiv 1 \pmod 5$. D'où le lemme.

1.2.2 Étude de la réduction de E en dehors de $\{2,5\}$

On démontre le résultat suivant :

Lemme 1.13 *Soit ℓ un nombre premier distinct de 2 et 5. La courbe E est semi-stable en ℓ et l'on a*

$$v_\ell(N_E) = \begin{cases} 1 & \text{si } \ell \text{ divise } cd, \\ 0 & \text{sinon.} \end{cases}$$

L'équation (1.6) définit un modèle minimal en ℓ de E et $\Delta_m = \Delta$. On a de plus,

$$v_\ell(\Delta_m) \equiv \begin{cases} 4v_\ell(d) \pmod p & \text{si } \ell \text{ divise } a+b, \\ 2v_\ell(d) \pmod p & \text{si } \ell \text{ ne divise pas } a+b. \end{cases} \tag{1.10}$$

En particulier,

$$p \text{ divise } v_\ell(\Delta_m) \Longleftrightarrow \ell \text{ ne divise pas } d. \tag{1.11}$$

Démonstration. D'après l'égalité,

$$\Delta = 2^4.5^3(a+b)^2(a^5+b^5)^2,$$

on a $v_\ell(\Delta) = 2v_\ell(a+b) + 2v_\ell(a^5+b^5)$. Or

$$a^5+b^5 = dc^p,$$

donc $v_\ell(a^5+b^5) = v_\ell(d) + pv_\ell(c)$. D'où

$$v_\ell(\Delta) \equiv 2v_\ell(a+b) + 2v_\ell(d) \pmod p. \tag{1.12}$$

Si ℓ ne divise pas cd, alors d'après l'égalité $a^5+b^5 = dc^p$ et le fait que $a+b$ divise a^5+b^5, ℓ ne divise pas Δ et E a donc bonne réduction en ℓ.

Supposons que ℓ divise cd. Dans ce cas, ℓ divise a^5+b^5. On distingue alors deux cas suivant que $a+b$ est ou non divisible par ℓ.

1. Supposons que ℓ divise $a + b$. Alors, $\phi(a, b) \equiv 5a^4 \pmod{\ell}$, d'après le lemme 1.10. On en déduit

$$c_4 \equiv 2^4.5^2a^4 \pmod{\ell}$$

d'où $v_\ell(c_4) = 0$. L'équation (1.6) est donc minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$ et $v_\ell(\Delta_m) = v_\ell(\Delta)$.
Puisque ℓ divise $a + b$, ℓ ne divise pas $\phi(a, b)$ (lemme 1.11). On en déduit

$$v_\ell(a + b) \equiv v_\ell(d) \pmod{p}.$$

La congruence (1.12) entraîne alors la condition (1.10). L'équivalence (1.11) en résulte vu que l'on a $0 \leq v_\ell(d) \leq 4$.

2. Supposons que ℓ ne divise pas $a + b$. On a $\phi(a, b) \equiv 0 \pmod{\ell}$ car ℓ divise $a^5 + b^5$ sans diviser $a + b$. D'après l'égalité (1.9), ℓ ne divise pas $a^2 + b^2$ car ℓ ne divise pas ab. On en déduit que $v_\ell(c_4) = 0$. Par suite, l'équation (1.6) est minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$. D'après la congruence (1.12), on a $v_\ell(\Delta_m) \equiv 2v_\ell(d) \pmod{p}$ et l'on conclut comme ci-dessus.

1.2.3 Étude de la réduction de E en 5

On démontre le résultat suivant :

Lemme 1.14 *La courbe E a mauvaise réduction de type additif en 5 et l'on a $v_5(N_E) = 2$. L'équation (1.6) est minimale en 5. L'invariant modulaire j de E est entier en 5 si et seulement si 5 ne divise pas $a + b$.*

De plus, p divise $v_5(j)$ si et seulement si l'une des deux conditions suivantes est satisfaite :

1. *on a $a + b \not\equiv 0 \pmod{5}$,*
2. *on a $a + b \equiv 0 \pmod{5}$ et $(p, v_5(d)) \in \{(7, 3), (11, 4)\}$.*

Démonstration. On distingue deux cas.

1. Supposons que 5 ne divise pas $a + b$. Dans ce cas, $\phi(a, b) \equiv 1 \pmod{5}$ car $a^5 + b^5 \equiv a + b \pmod{5}$, d'où :

$$(v_5(c_4), v_5(c_6), v_5(\Delta)) = (1, \geq 2, 3).$$

Le type de Kodaira de E est donc III (cf. tableau I, p.126 de [Pap93]) et l'on a ainsi $v_5(N_E) = 2$. L'égalité $j = c_4^3/\Delta$ entraîne alors $v_5(j) = 0$.

2. Supposons que 5 divise $a + b$. On a alors (lemme 1.10)

$$a^2 + b^2 \equiv -2ab \pmod{25} \quad \text{et} \quad \phi(a, b) \equiv 5a^2b^2 \pmod{25}.$$

On a donc :

$$\frac{c_4}{5} \equiv 2^4.5a^2b^2 \pmod{25} \quad \text{et} \quad \frac{c_6}{5^2} \equiv 2^6.5(ab)^3 \pmod{25},$$

d'où les égalités :

$$v_5(c_4) = 2 \quad \text{et} \quad v_5(c_6) = 3.$$

On en conclut que la courbe E a mauvaise réduction de type additif en 5 et que l'équation (1.6) est minimale en 5. Le type de Kodaira de E est donc I_ν^* où $\nu = 4v_5(a+b) - 1$ et l'on obtient $v_5(N_E) = 2$ (cf. *loc. cit.*).
D'après le lemme 1.11, on a :

$$v_5(a^5 + b^5) = v_5(a+b) + 1,$$

d'où $v_5(\Delta) = 5 + 4v_5(a+b) \geq 9$ et l'inégalité $v_5(j) < 0$.
De l'égalité

$$v_5(\Delta) = 5 + 4(v_5(d) + pv_5(c) - 1),$$

il vient :

$$v_5(j) = 6 - v_5(\Delta) \equiv 5 - 4v_5(d) \pmod{p}.$$

Autrement dit,

$$v_5(j) \equiv \begin{cases} 5 \pmod{p} & \text{si } v_5(d) = 0, \\ 1 \pmod{p} & \text{si } v_5(d) = 1, \\ -3 \pmod{p} & \text{si } v_5(d) = 2, \\ -7 \pmod{p} & \text{si } v_5(d) = 3, \\ -11 \pmod{p} & \text{si } v_5(d) = 4. \end{cases}$$

Cela établit le lemme.

1.2.4 Étude de la réduction de E en 2 si d est impair

On démontre le résultat suivant :

Lemme 1.15 *Supposons d impair. La courbe E a mauvaise réduction en 2.*

1. *Si a est pair, E a réduction de type additif en 2. On a*

$$v_2(N_E) = \begin{cases} 4 & \text{si } v_2(a) = 1, \\ 3 & \text{si } v_2(a) \geq 2. \end{cases}$$

2. *Si a est impair, E a réduction de type multiplicatif en 2 et l'on a alors $v_2(N_E) = 1$.*

L'équation (1.6) est minimale en 2 si et seulement si a est pair.

Démonstration. On est amené à distinguer deux cas suivant la parité de a.

1. Supposons a pair. On a alors :

$$v_2(c_4) \geq 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

En fait, on a plus précisément $(v_2(a), v_2(c_4)) \in \{(1, \geq 6), (\geq 2, 5)\}$. En effet, on a

$$\begin{aligned} \frac{c_4}{2^4} \equiv 2 + 3ab^3 &\equiv 2 + 3ab \pmod{4} \\ &\equiv \begin{cases} 0 \pmod{4} & \text{si} \quad v_2(a) = 1 \\ 2 \pmod{4} & \text{si} \quad v_2(a) \geq 2. \end{cases} \end{aligned} \tag{1.13}$$

Il convient donc de séparer les cas où $v_2(a) = 1$ et $v_2(a) \geq 2$.

(a) Supposons $v_2(a) = 1$. On est dans le cas 3 ou 5 de Tate (cf. tableau IV, p.129 de [Pap93]). D'après la proposition 1, p.124 de *loc. cit.* appliquée avec $r = t = 1$, on est dans un cas ≥ 4 si et seulement si

$$5\left(\frac{a^5+b^5}{a+b}\right) - 5(a^2+b^2) \equiv 0 \pmod 4,$$

ce qui équivaut à

$$a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2+b^2) \equiv 0 \pmod 4.$$

Or on a $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2+b^2) \equiv -ab \pmod 4$ et comme $v_2(a) = 1$, l'entier ab n'est pas multiple de 4. On est donc dans le cas 3 de Tate et l'on a $v_2(N_E) = 4$.

(b) Supposons $v_2(a) \geq 2$. On a alors :

$$v_2(c_4) = 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

On est donc dans le cas 3 ou 4 de Tate. On déduit alors de la congruence $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2+b^2) \equiv -ab \pmod 4$, que l'on est dans le cas 4 de Tate et l'on a $v_2(N_E) = 3$.

2. Supposons a impair. Dans ce cas, d'après la remarque préliminaire 4, b est impair et c est pair. On a ainsi $\phi(a,b) \equiv 1 \pmod 2$, $a^2+b^2 \equiv 2 \pmod 4$ et l'égalité $v_2(a^5+b^5) = v_2(a+b)$. Compte tenu de l'égalité (1.1), il en résulte que l'on a

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, \geq 32).$$

Vérifions que l'équation (1.6) n'est pas minimale en 2. On étudie pour cela la congruence de $c_6/2^6$ modulo 4 ([Kra89, p.77]). On constate que l'on a

$$\frac{c_6}{2^6} \equiv 2ab + 1 \pmod 4.$$

Puisque ab est impair, on a $ab \equiv \pm 1 \pmod 4$, et l'on obtient la congruence $c_6/2^6 \equiv -1 \pmod 4$. Notre assertion résulte alors du corollaire du théorème 2 de *loc. cit.*. On en déduit que E a réduction multiplicative en 2 et l'on a donc $v_2(N_E) = 1$.

Cela termine la démonstration du lemme 1.15.

1.2.5 Étude de la réduction de E en 2 si d est pair

On démontre le résultat suivant :

Lemme 1.16 *Supposons d pair.*

1. *Si c est impair et si $v_2(d) = 2$, E a bonne réduction en 2, auquel cas on a $v_2(N_E) = 0$.*
2. *Si c est impair et si $v_2(d) = 1$, E a mauvaise réduction de type additif en 2 et l'on a $v_2(N_E) = 4$.*
3. *Supposons c pair ou bien que l'on ait $v_2(d) = 3$ ou 4. Alors E a réduction de type multiplicatif en 2 et l'on a $v_2(N_E) = 1$.*

L'équation (1.6) est minimale en 2 si et seulement si c est impair et $v_2(d) = 1$.

Démonstration. Puisque d est pair, les entiers a et b sont impairs. On a donc $\phi(a,b) \equiv 1 \pmod 2$ et $v_2(a+b) = v_2(a^5+b^5)$. Il en résulte que l'on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \quad v_2(\Delta) = 4(1 + v_2(d) + pv_2(c)).$$

En particulier, on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, \geq 8).$$

Plus précisément, on a

$$\begin{cases} v_2(\Delta) = 8 & \text{si} \quad v_2(d) = 1 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) = 12 & \text{si} \quad v_2(d) = 2 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) > 12 & \text{si} \quad v_2(d) = 3 \text{ ou } 4, \text{ ou bien si } c \text{ est pair.} \end{cases}$$

On distingue donc les cas où $v_2(\Delta) = 8$ et $v_2(\Delta) \geq 12$.

1. Supposons $v_2(\Delta) \geq 12$. On a comme ci-dessus les congruences

$$\frac{c_6}{2^6} \equiv 2ab + 1 \equiv -1 \pmod 4.$$

Par suite, l'équation (1.6) n'est pas minimale en 2. Si l'on a $v_2(d) = 2$ et si c est impair, la courbe E a donc bonne réduction en 2, i.e. on a $v_2(N_E) = 0$. Par ailleurs, si $v_2(d) = 3$ ou 4, ou bien si c est pair, E a réduction multiplicative en 2 et l'on a $v_2(N_E) = 1$.

2. Supposons $v_2(\Delta) = 8$. On a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 8)$$

et l'on est dans le cas 6, 7 ou 8 de Tate. D'après la proposition 3 p.124 de [Pap93], on est amené à déterminer si la congruence

$$-5^2\left(\frac{a^5+b^5}{a+b}\right)^2 + 2.3.5r^2\left(\frac{a^5+b^5}{a+b}\right) - 2^2.5r^3(a^2+b^2) + 3r^4 \equiv 0 \pmod{32}$$

a ou non une solution $r \in \mathbf{Z}$. On vérifie que $r = 1$ convient. D'après la proposition 3 de *loc. cit.*, il existe $t \in \mathbf{Z}$ tel que

$$5\left(\frac{a^5+b^5}{a+b}\right) - 5(a^2+b^2) + 1 \equiv t^2 \pmod 8,$$

et l'on vérifie que $t = 2$ convient. Posons

$$u = 5\left(\frac{a^5+b^5}{a+b}\right) - 5(a^2+b^2) - 3.$$

Vérifions que l'on a $v_2(u) = 3$. Les entiers a^2 et b^2 sont congrus à 1 ou 9 modulo 16, de sorte que l'on a $a^2 \equiv b^2 \pmod{16}$ ou $b^2 \equiv 9a^2 \pmod{16}$. Par ailleurs, on a $v_2(d) = 1$ et c est impair. D'après l'égalité (1.1), on a donc la congruence $a \equiv b \pmod 4$, autrement dit, on a $ab \equiv 1$ ou $5 \pmod 8$.

(a) Supposons $a^2 \equiv b^2 \pmod{16}$. Dans ce cas, on vérifie que l'on a

$$u \equiv 2 + 6ab \pmod{16}.$$

D'après l'hypothèse faite, on a $ab \equiv 1 \pmod{8}$, ce qui entraîne notre assertion.

(b) Supposons $b^2 \equiv 9a^2 \pmod{16}$. On obtient alors

$$u \equiv 2(1 - ab) \pmod{16}.$$

Par ailleurs, on a dans ce cas $ab \equiv 5 \pmod{8}$, d'où l'assertion.

Il en résulte que l'on est dans le cas 6 de Tate, puis que $v_2(N_E) = 4$. D'où le lemme 1.16.

Les propositions 1.7, 1.8 et 1.9 résultent alors des lemmes 1.13 à 1.16.

1.3 La représentation ρ_p^E

Soit p un nombre premier ≥ 7 et (a, b, c) un élément de $S_p(d)$. Notons $\overline{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ le groupe de Galois absolu de $\mathbf{Q}$. Soit $E[p]$ le sous-groupe de $E(\overline{\mathbf{Q}})$ constitué des points de p-torsion de la courbe elliptique E. C'est un $\mathbf{F}_p$-espace vectoriel de dimension 2 sur lequel $\mathrm{G}_{\mathbf{Q}}$ opère continûment. Par le choix d'une base de $E[p]$ sur $\mathbf{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^E : \mathrm{G}_{\mathbf{Q}} \longrightarrow \mathbf{GL}_2(\mathbf{F}_p).$$

À une telle représentation J.-P. Serre associe un poids k qui est un entier ≥ 2 et un conducteur $N(\rho_p^E)$ qui est un entier ≥ 1, premier à p, qui divise le conducteur N_E de E (cf. [Ser87]).

Proposition 1.17 *La représentation ρ_p^E est irréductible.*

Démonstration. La courbe E a un point d'ordre deux rationnel sur $\mathbf{Q}$. Par suite, si ρ_p^E était réductible, le groupe $E(\overline{\mathbf{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $\mathrm{G}_{\mathbf{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbf{Q}$. Or, si $p \geq 11$, B. Mazur et M. A. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbf{Q})$ est vide (cf. [Ken82]). D'où le résultat dans ce cas.

Supposons maintenant $p = 7$ et ρ_7^E réductible. La courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [Cre97] ([Lig75, p.45]). Elle possède exactement deux points rationnels sur $\mathbf{Q}$ qui correspondent aux deux classes de $\overline{\mathbf{Q}}$-isomorphisme de courbes elliptiques d'invariants $j = -15^3$ et 255^3. Ce sont en effet les invariants modulaires des courbes notées 49A1 et 49A2 dans les tables de [Cre97] et elles ont bien un sous-groupe d'ordre 14 stable par $\mathrm{G}_{\mathbf{Q}}$. La courbe elliptique E correspond donc à un point rationnel sur $\mathbf{Q}$ de la courbe modulaire $Y_0(14)$. En particulier, on a $j = -15^3$ ou 255^3. En posant $t = a/b$, on en déduit que t est une solution rationnelle de l'équation :

$$2^8 \frac{(2t^4 + 3t^3 + 7t^2 + 3t + 2)^3}{(t+1)^2(t^5+1)^2} = -15^3 \quad \text{ou} \quad 255^3.$$

On vérifie que cela conduit à une contradiction. D'où la proposition.

Proposition 1.18 *On a $k = 2$ si p ne divise pas d et $k = p + 1$ sinon.*

Démonstration. Supposons que p ne divise pas d. Si p ne divise pas c, alors E a bonne réduction en p (lemme 1.13) et l'on a $k = 2$ d'après la proposition 5 p.191 de [Ser87]. Si p divise c, puisque l'on a $p \geq 7$, la courbe E a réduction multiplicative en p (*loc. cit.*). Par ailleurs, p divise $v_p(\Delta_m)$ (*loc. cit.*), ce qui entraîne de nouveau $k = 2$.

Supposons que p divise d. D'après le lemme 1.13, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_m)$. Cela conduit à $k = p + 1$, d'où le résultat.

Calcul de $N(\rho_p^E)$. Posons

$$r' = \prod_{\substack{\ell \neq 2,5,p \\ \ell | d}} \ell,$$

où ℓ parcourt les diviseurs premiers de d distincts de $2, 5$ et p. Le conducteur $N(\rho_p^E)$ de ρ_p^E est donné dans les deux énoncés suivants :

Proposition 1.19 *Supposons d* impair. *Alors :*

1. $N(\rho_p^E) = 2^4.5^2 r'$, *si* $v_2(a) = 1$;
2. $N(\rho_p^E) = 2^3.5^2 r'$, *si* $v_2(a) \geq 2$;
3. $N(\rho_p^E) = 2.5^2 r'$, *si a est impair.*

Proposition 1.20 *Supposons d* pair. *Alors :*

1. $N(\rho_p^E) = 2.5^2 r'$, *si* $v_2(d) = 3$ *ou* 4 ;
2. $N(\rho_p^E) = 5^2 r'$, *si* $v_2(d) = 2$;
3. $N(\rho_p^E) = 2.5^2 r'$, *si* $v_2(d) = 1$ *et c est pair.*
4. $N(\rho_p^E) = 2^4.5^2 r'$, *si* $v_2(d) = 1$ *et c est impair.*

Avant de démontrer ces propositions, on commence par le résultat suivant.

Lemme 1.21 *Supposons que E ait réduction de type multiplicatif en 2. Alors,*

$$v_2(\Delta_m) \equiv -8 + 4v_2(d) \pmod{p}. \tag{1.14}$$

En particulier, p divise $v_2(\Delta_m)$ si et seulement si c est pair et $v_2(d) = 2$.

Démonstration. Puisque E a réduction de type multiplicatif en 2, on est dans l'un des cas suivants (lemmes 1.15 et 1.16) :

1. les entiers d et a sont impairs (et c est pair) ;
2. les entiers d et c sont pairs ;
3. l'entier c est impair et l'on a $v_2(d) = 3$ ou 4.

Dans chacun des trois cas ci-dessus, l'entier ab est impair donc

$$v_2(a + b) = v_2(a^5 + b^5).$$

D'après la proposition 1.7, on a :

$$\Delta_m = \frac{\Delta}{2^{12}}.$$

On en déduit

$$v_2(\Delta_m) = 4 + 4v_2(a^5 + b^5) - 12.$$

Or $v_2(a^5 + b^5) = v_2(d) + pv_2(c) \equiv v_2(d) \pmod{p}$. D'où la congruence (1.14). L'équivalence du lemme s'en déduit immédiatement car on a $0 \leq v_2(d) \leq 4$.

Démontrons à présent les propositions 1.19 et 1.20. Puisque $N(\rho_p^E)$ divise N_E, pour tout nombre premier ℓ qui ne divise pas $10r$, on a $v_\ell(N(\rho_p^E)) = 0$.

Considérons un diviseur premier ℓ de N_E distinct de $2, 5$ et p. D'après le lemme 1.13 et [Kra97a, p.28], on a

$$v_\ell(N(\rho_p^E)) = \begin{cases} 1 & \text{si } \ell \text{ divise } d, \\ 0 & \text{sinon.} \end{cases}$$

La courbe E ayant réduction de type additif en 5, on a $v_5(N(\rho_p^E)) = 2$ (*loc. cit.*).

Il reste à déterminer l'exposant de 2 dans $N(\rho_p^E)$. La valeur de l'exposant de 2 dans le conducteur N_E est donnée dans les propositions 1.8 et 1.9. Dans le cas où E a réduction de type additif en 2, i.e. si $v_2(N_E) \geq 2$, on a $v_2(N(\rho_p^E)) = v_2(N_E)$ (*loc. cit.*). Si E a réduction multiplicative en 2, alors d'après le lemme 1.21, $v_2(N(\rho_p^E)) = v_2(N_E)$ sauf si c est pair et $v_2(d) = 2$ auquel cas on a $v_2(N(\rho_p^E)) = v_2(N_E) - 1$, i.e. $v_2(N(\rho_p^E)) = 0$.

Compte tenu du fait que $N(\rho_p^E)$ est premier à p, cela termine la démonstration des propositions 1.19 et 1.20.

1.4 Démonstrations des résultats

On suppose pour toute la suite qu'il existe un élément $(a, b, c) \in S_p(d)$ où p est un nombre premier ≥ 7. Soit E la courbe d'équation (1.6) attachée à la solution (a, b, c).

Notations. Si n est un entier ≥ 1, on note $\mathcal{S}_2^+(n)$ le $\mathbf{C}$-espace vectoriel formé des newforms paraboliques de poids 2 pour le sous-groupe $\Gamma_0(n)$ au sens de [AL70].

La représentation ρ_p^E est irréductible, de poids 2 et de conducteur $N(\rho_p^E)$. D'après les travaux de K. Ribet (cf. [Rib90]), il existe alors une newform

$$f = q + \sum_{n \geq 2} a_n(f) q^n \in \mathcal{S}_2^+(N(\rho_p^E)) \quad \text{avec} \quad q = e^{2i\pi\tau},$$

et une place $\mathfrak{P}$ de $\overline{\mathbf{Q}}$ de caractéristique résiduelle p telles que, pour tout nombre premier ℓ, on ait :

$$\begin{cases} a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{P}} & \text{si } \ell \text{ ne divise pas } pN_E, \\ a_\ell(f) \equiv \pm(\ell + 1) \pmod{\mathfrak{P}} & \text{si } \ell \text{ divise } N_E \text{ et ne divise pas } pN(\rho_p^E). \end{cases} \tag{1.15}$$

Par ailleurs, dans le cas où les coefficients $a_n(f)$ sont dans $\mathbf{Z}$, la newform f correspond à une courbe elliptique $A/\mathbf{Q}$ de conducteur $N(\rho_p^E)$ unique à isogénie près. Notons respectivement

$$L_E(s) = \sum_{n \geq 1} a_n(E) n^{-s} \quad \text{et} \quad L_A(s) = \sum_{n \geq 1} a_n(A) n^{-s}$$

les fonctions L de Hasse - Weil de E et A.

Les représentations ρ_p^E et ρ_p^A sont alors isomorphes et l'on a en particulier :

$$a_\ell(E) \equiv a_\ell(A) \pmod{p}, \tag{1.16}$$

pour tout nombre premier ℓ ne divisant pas N_E (cf. [KO92]). Il s'agit de contredire l'existence de f.

Soit $\mathbf{Q}(E[p])/\mathbf{Q}$ l'extension de $\mathbf{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbf{Q}$. On note e son indice de ramification en 5.

Le lemme suivant intervient dans les paragraphes 1.4.3 et 1.4.4.

Lemme 1.22 *1. Si 5 divise $a+b$, on a :*

$$e = \begin{cases} 2 & \text{si } (p, v_5(d)) = (7,3) \text{ ou } (11,4), \\ 2p & \text{sinon.} \end{cases} \tag{1.17}$$

2. Si 5 ne divise pas $a+b$, on a $e = 4$.

Démonstration. Si 5 divise $a+b$, la courbe E a potentiellement réduction multiplicative en 5, autrement dit, E a réduction additive en 5 et son invariant modulaire n'est pas entier en 5 (lemme 1.14). L'égalité (1.17) résulte alors du lemme 1.14 et de [CK02, p.7].

Si 5 ne divise pas $a+b$, l'invariant modulaire j de E est entier en 5 (lemme 1.14). La courbe E a donc potentiellement bonne réduction en 5. La valuation en 5 de son discriminant minimal vaut 3 (cf. §1.2.3). Le défaut de semi-stabilité en 5 de E (qui est mesuré par l'ordre d'un certain groupe fini Φ_5) est donc d'ordre 4 ([Ser72, p.312]), d'où le résultat.

1.4.1 Démonstration du théorème 1.2

On suppose ici que l'on a $d = 1$ et que c est pair. L'entier a est impair. D'après l'étude faite dans la partie 1.3, la représentation ρ_p^E est irréductible de poids 2 et de conducteur 50. Or une base du $\mathbf{C}$-espace vectoriel $\mathcal{S}_2^+(50)$ correspond aux deux courbes elliptiques sur $\mathbf{Q}$ de conducteur 50 notées 50A1 et 50B1 dans [Cre97] et d'équations respectives :

$$\begin{aligned} 50\text{A1} : y^2 + xy + y &= x^3 - x - 2, \\ 50\text{B1} : y^2 + xy + y &= x^3 + x^2 - 3x + 1. \end{aligned}$$

On va alors contredire les congruences (1.15) avec le nombre premier $\ell = 3$. On remarque pour cela que l'on a

$$\begin{cases} a_3(50\text{A1}) &= +1, \\ a_3(50\text{B1}) &= -1. \end{cases}$$

Par ailleurs, la courbe elliptique E a réduction semi-stable en 3 (lemme 1.13). Supposons que E ait réduction multiplicative en 3. Puisque 3 divise N_E, mais pas $50p = pN(\rho_p^E)$, on déduit des congruences (1.15) que l'on a

$$\pm 1 \equiv \pm 4 \pmod{p},$$

ce qui conduit à une contradiction car $p \geq 7$. La courbe E a donc bonne réduction en 3. Puisque E a un point d'ordre 2 rationnel sur $\mathbf{Q}$, $a_3(E)$ est pair et l'inégalité $|a_3(E)| < 2\sqrt{3}$ ([Sil92, th.1.1, p.131]) entraîne $a_3(E) = 0$ ou ± 2. D'après les congruences (1.15), on a donc

$$\pm 1 \equiv a_3(E) \pmod{p},$$

ce qui conduit de nouveau à une contradiction. Cela termine la démonstration du théorème 1.2.

1.4.2 Démonstration du théorème 1.3

On a $r' = 1$. On distingue deux cas suivant la valeur de $v_2(d)$.

1. Supposons $v_2(d) = 2$. D'après la proposition 1.20, on a $N(\rho_p^E) = 25$. Or l'espace $\mathcal{S}_2^+(25)$ est réduit à 0. D'où le théorème dans ce cas.
2. Supposons $v_2(d) = 3$ ou 4. Dans ce cas, on a $N(\rho_p^E) = 50$, ce qui entraîne, par le même argument que celui utilisé dans le §1.4.1, le résultat.

1.4.3 Démonstration du théorème 1.4

Supposons que l'on soit dans le cas où les coefficients $a_n(f)$ sont dans $\mathbf{Z}$. Les congruences (1.16) sont réalisées. On utilise ici la méthode symplectique reposant sur le lemme suivant ([HK02, p.180]). Notons $\Delta_m(A)$ le discriminant minimal de A.

Lemme 1.23 *Soient ℓ_1 et ℓ_2 deux nombres premiers distincts, autres que p. Supposons que E et A aient réduction de type multiplicatif en ℓ_i et que p ne divise pas $v_{\ell_i}(\Delta_m)$, auquel cas p ne divise pas non plus $v_{\ell_i}\big(\Delta_m(A)\big)$ $(i = 1, 2)$. Alors, les classes modulo p de $v_{\ell_1}(\Delta_m)v_{\ell_2}(\Delta_m)$ et $v_{\ell_1}\big(\Delta_m(A)\big)v_{\ell_2}\big(\Delta_m(A)\big)$ diffèrent multiplicativement par un carré de $\mathbf{F}_p$.*

On suppose ici que d s'écrit

$$d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma, \quad \text{avec } \alpha = 3 \text{ ou } 4 \quad \text{et} \quad 1 \leq \beta \leq 4,\ 0 \leq \gamma \leq 4.$$

D'après la proposition 1.20, on a alors :

$$N(\rho_p^E) \quad = \quad 150.$$

Une base de $\mathcal{S}_2^+(150)$ correspond aux trois classes d'isogénie de courbes elliptiques sur $\mathbf{Q}$ de conducteur 150. Ainsi ρ_p^E est isomorphe à la représentation de $\mathrm{G}_{\mathbf{Q}}$ dans les points de p-torsion de l'une des courbes notées 150A1, 150B1 et 150C1 dans les tables de [Cre97]. Par ailleurs, E a réduction multiplicative en 2 et 3 (lemmes 1.13 et 1.16) et d'après le lemme 1.21, on a donc :

$$v_2(\Delta_m) \equiv \begin{cases} 4 \pmod{p} & \text{si } \alpha = 3 \\ 8 \pmod{p} & \text{si } \alpha = 4. \end{cases} \tag{1.18}$$

D'après le lemme 1.12, 3 divise $a + b$ et d'après le lemme 1.13, on a donc :

$$v_3(\Delta_m) \equiv 4\beta \pmod{p}. \tag{1.19}$$

Les entiers $v_2(\Delta_m)$ et $v_3(\Delta_m)$ ne sont pas divisibles par p.

On distingue alors deux cas suivant la valeur de l'entier α.

Supposons $\alpha = 3$

On distingue deux cas selon que 5 divise on non $a + b$.

1. Supposons que 5 divise $a + b$. Démontrons que l'on a les assertions suivantes :
$$\begin{cases} 3 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4, \\ 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 2. \end{cases} \tag{1.20}$$
D'après le lemme 1.22, l'indice de ramification en 5 de l'extension $\mathbf{Q}(E[p])/\mathbf{Q}$ est 2 ou $2p$. Or les courbes notées 150A1 et 150B1 dans [Cre97] ont réduction additive en 5 et leurs invariants modulaires sont entiers en 5. Les valuations de leurs discriminants minimaux en 5 sont respectivement 3 et 9. L'indice de ramification en 5 des extensions de $\mathbf{Q}$ engendrées par leurs points de p-torsion vaut donc 4 ([Ser72, p.312]). Puisque l'on a $p \neq 2$, cela entraîne que ρ_p^E est isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [Cre97]. On applique alors le résultat du lemme 1.23 avec les courbes E et A, et les nombres premiers $\ell_1 = 2$, $\ell_2 = 3$. On a $v_2(\Delta_m(A)) = 4$ et $v_3(\Delta_m(A)) = 3$. D'après (1.18) et (1.19), on obtient ainsi :
$$3 \pmod p \equiv \beta \pmod p \pmod{(\mathbf{F}_p^*)^2},$$
d'où les assertions (1.20).

2. Supposons que 5 ne divise pas $a + b$. Dans ce cas, vérifions que l'on a :
$$\begin{cases} 2 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases} \tag{1.21}$$
L'invariant modulaire de E est entier en 5. D'après le lemme 1.22, l'indice de ramification en 5 de l'extension $\mathbf{Q}(E[p])/\mathbf{Q}$ est 4. Or la courbe elliptique notée 150C1 a un invariant modulaire non entier en 5. Comme ci-dessus, on en déduit que ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [Cre97]. On a $v_2(\Delta_m(A)) = 2$ et $v_3(\Delta_m(A)) = 1$. D'après le lemme 1.23 et les congruences (1.18) et (1.19), on obtient :
$$2 \pmod p \equiv \beta \pmod p \pmod{(\mathbf{F}_p^*)^2},$$
d'où les assertions (1.21).

Démontrons le théorème 1.4 si $\alpha = 3$. Supposons $\gamma \geq 1$. Dans ce cas, d'après le lemme 1.12, 5 divise $a + b$. Par hypothèse, on a $\beta \in \{1, 2, 4\}$. Par ailleurs, on a les équivalences :
$$3 \pmod p \notin (\mathbf{F}_p^*)^2 \iff p \equiv 5 \text{ ou } 7 \pmod{12}, \tag{1.22}$$
et
$$6 \pmod p \notin (\mathbf{F}_p^*)^2 \iff p \equiv 7, 11, 13 \text{ ou } 17 \pmod{24}, \tag{1.23}$$
d'où le résultat dans ce cas.

Supposons $\gamma = 0$, i.e. 5 ne divise pas d. On a alors $\beta = 1$ ou 4. Et, d'après ce qui précède, 2 (mod p) ou 3 (mod p) appartient à $(\mathbf{F}_p^*)^2$ suivant que 5 divise ou non $a + b$.

De l'équivalence

$$2 \pmod p \notin (\mathbf{F}_p^*)^2 \iff p \equiv 3 \text{ ou } 5 \pmod 8, \tag{1.24}$$

on déduit :

$$3 \pmod p \notin (\mathbf{F}_p^*)^2 \text{ et } 2 \pmod p \notin (\mathbf{F}_p^*)^2 \iff p \equiv 5 \text{ ou } 19 \pmod{24}. \tag{1.25}$$

Compte tenu des deux alinéas précédents, cela prouve le théorème 1.4 si $\alpha = 3$.

Supposons $\alpha = 4$

La démarche est identique à celle du paragraphe précédent : seules les congruences obtenues diffèrent. On explicitera donc les calculs sans répéter exhaustivement les raisonnements.

1. Supposons que 5 divise $a + b$. La représentation ρ_p^E est alors isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [Cre97]. On déduit du lemme 1.23 les congruences :

$$3 \pmod p \equiv 2\beta \pmod p \pmod{(\mathbf{F}_p^*)^2}.$$

Autrement dit, on a :

$$\begin{cases} 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 3 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 2 \\ 2 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases}$$

2. Supposons que 5 ne divise pas $a + b$. On sait qu'alors ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [Cre97]. On obtient dans ce cas :

$$\beta \pmod p \in (\mathbf{F}_p^*)^2.$$

Démontrons alors le théorème 1.4 si $\alpha = 4$.

Supposons $\gamma = 0$, i.e. 5 ne divise pas d. Alors par hypothèse $\beta = 2$ ou 3. D'après les alinéas ci-dessus, 2 (mod p) ou 3 (mod p) appartient à $(\mathbf{F}_p^*)^2$. D'où le résultat dans ce cas, d'après la congruence (1.25).

Supposons $\gamma \geq 1$. Alors 5 divise $a + b$ et $\beta \in \{1, 2, 3, 4\}$. Si $\beta = 1$ ou 4, on a le résultat avec la congruence (1.23). Les cas où $\beta = 2$ et $\beta = 3$ se déduisent respectivement des congruences (1.22) et (1.24).

Ceci achève la démonstration du théorème 1.4.

1.4.4 Démonstration du théorème 1.5

On rappelle que p est un nombre premier ≥ 7, (a, b, c) est un élément de $S_p(3)$ et que E la courbe d'équation (1.6) attachée à (a, b, c).

D'après la proposition 1.19, on a :

$$N(\rho_p^E) = \begin{cases} 150 & \text{si } a \text{ est impair;} \\ 600 & \text{si } v_2(a) \geq 2; \\ 1200 & \text{si } v_2(a) = 1. \end{cases}$$

Les newforms appartenant aux espaces $\mathcal{S}_2^+(150)$, $\mathcal{S}_2^+(600)$ et $\mathcal{S}_2^+(1200)$ sont toutes à coefficients entiers relatifs. Elles correspondent donc à des courbes elliptiques. Il y a en trois de conducteur 150, neuf de conducteur 600 et dix-neuf de conducteur 1200, soit trente-et-une courbes au total. Par commodité pour le lecteur, on donne en Appendice la liste des équations de ces courbes elliptiques ainsi que la valeur des invariants dont on aura besoin.

On considère les deux ensembles de courbes elliptiques suivants, avec les notations des tables de [Cre97] :

$$\begin{aligned} \mathcal{F}_1 &= \{150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{E1}, 1200\text{G1}, 1200\text{J1}, 1200\text{P1}\}; \\ \mathcal{F}_2 &= \{150\text{A1}, 150\text{B1}, 600\text{C1}, 600\text{H1}, 1200\text{B1}, 1200\text{I1}, 1200\text{M1} \\ &\quad 1200\text{N1}, 1200\text{Q1}, 1200\text{S1}\}. \end{aligned}$$

Le lemme suivant décrit les isomorphismes possibles entre ρ_p^E et les représentations ρ_p^A où A est l'une des trente-et-une courbes elliptiques de conducteur 150, 600 et 1200.

Lemme 1.24 *1. Si 5 divise $a+b$, alors il existe A dans $\mathcal{F}_1$ tel que ρ_p^E soit isomorphe à ρ_p^A ;*

2. Si 5 ne divise pas $a+b$, alors il existe A dans $\mathcal{F}_2$ tel que ρ_p^E soit isomorphe à ρ_p^A.

Démonstration. La représentation ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique A de conducteur 150, 600 ou 1200. Définissons l'ensemble suivant :

$$\begin{aligned} \mathcal{G} &= \{150\text{A1}, 150\text{B1}, 600\text{B1}, 600\text{C1}, 600\text{D1}, 600\text{E1}, 600\text{G1}, 600\text{H1}, 600\text{I1}, \\ &\quad 1200\text{A1}, 1200\text{B1}, 1200\text{C1}, 1200\text{D1}, 1200\text{F1}, 1200\text{H1}, 1200\text{I1}, 1200\text{K1}, \\ &\quad 1200\text{L1}, 1200\text{M1}, 1200\text{N1}, 1200\text{O1}, 1200\text{Q1}, 1200\text{R1}, 1200\text{S1}\}. \end{aligned}$$

D'après le tableau 1.2 de l'Appendice, l'ensemble $\mathcal{G}$ (resp. $\mathcal{F}_1$) correspond précisément aux courbes de conducteur 150, 600 et 1200 ayant un invariant modulaire j entier en 5 (resp. non entier en 5).

On rappelle que la courbe E a réduction additive en 5 (lemme 1.14).

1. Supposons tout d'abord que 5 divise $a+b$. D'après le lemme 1.22, l'indice de ramification en 5 de l'extension $\mathbf{Q}(E[p])/\mathbf{Q}$ est $2p$ (car $v_5(d) \neq 3, 4$). Or les courbes de l'ensemble $\mathcal{G}$ ont toutes réduction additive en 5 et leur invariant modulaire est entier en 5. Leur défaut de semi-stabilité en 5 est alors d'ordre 2, 3, 4 ou 6 (cf. le tableau 1.2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune des courbes de l'ensemble $\mathcal{G}$. Autrement dit, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_1$.

2. Supposons que 5 ne divise pas $a+b$. L'invariant modulaire de E est entier en 5 (lemme 1.14). D'après le lemme 1.22, l'indice de ramification en 5 de l'extension $\mathbf{Q}(E[p])/\mathbf{Q}$ est 4. Or les courbes A de l'ensemble $\mathcal{F}_1$ ont toutes réduction additive en 5 et leur invariant modulaire n'est pas entier en 5. L'indice de ramification en 5 de l'extension $\mathbf{Q}(A[p])/\mathbf{Q}$ est alors $2p$ (cf. tableau 1.2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune de ces courbes.

   Par ailleurs, parmi les courbes de l'ensemble $\mathcal{G}$, seules celles de l'ensemble $\mathcal{F}_2$ ont un défaut de semi-stabilité en 5 d'ordre 4. On en déduit que dans ce cas, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_2$.

Ceci achève la démonstration du lemme 1.24.

Remarque. Parmi les courbes des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$ du début du paragraphe, les courbes suivantes ont le même invariant modulaire j :

- 150C1 et 1200P1,
- 600A1 et 1200E1,
- 600F1 et 1200G1,
- 150A1, 150B1, 1200M1 et 1200Q1,
- 600C1, 600H1, 1200B1 et 1200I1,
- 600D1 et 1200A1,
- 1200N1 et 1200S1.

Leur invariant modulaire étant différent de 0 et de 1728, elles sont donc isomorphes sur une extension quadratique de $\mathbf{Q}$. L'ensemble $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) du théorème 1.5 est un ensemble de représentants des classes d'isomorphisme des courbes de l'ensemble $\mathcal{F}_1$ (resp. $\mathcal{F}_2$).

En particulier, pour toute courbe A de l'ensemble $\mathcal{F}_1$ (resp. $\mathcal{F}_2$), il existe une unique courbe F de l'ensemble $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) de même invariant modulaire que A. On a alors pour tout nombre premier ℓ :

$$a_\ell(A)^2 = a_\ell(F)^2. \tag{1.26}$$

Montrons à présent le théorème 1.5. D'après le lemme 1.24, ρ_p^E est isomorphe à ρ_p^A où A est une courbe des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$. On note F l'unique courbe elliptique des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ de même invariant modulaire que A. Soit alors n un entier ≥ 2 tel que le couple (F, n) vérifie la condition 1 du théorème 1.5 si A appartient à $\mathcal{F}_1$ et la condition 2 si A appartient à $\mathcal{F}_2$. On a le résultat suivant.

Lemme 1.25 *La courbe E a bonne réduction en q. Autrement dit, q ne divise pas c.*

Démonstration. Supposons que ce ne soit pas le cas. Dans ce cas, q divise c et d'après le lemme 1.13, la courbe E a réduction multiplicative en q. Comme A a bonne réduction en q, il vient d'après [KO92, prop.3(iii)] :

$$a_q(A) \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

Or, d'après (1.26), on a $a_q(A)^2 = a_q(F)^2$. C'est en contradiction avec les hypothèses du thèorème. D'où le lemme.

Désignons par $\overline{a}$ et $\overline{b}$ les réductions de a et b modulo q. On distingue à présent deux cas.

1. Supposons que 5 divise $a+b$, i.e. $F \in \mathcal{E}_1$. D'après les lemmes 1.11 et 1.12, il existe c_1 et c_2 deux entiers tels que :

$$5(a+b) = 3c_1^p, \quad \phi(a,b) = 5c_2^p \quad \text{et} \quad c = c_1 c_2.$$

De plus d'après le lemme 1.25, q ne divise pas c, ainsi

$$u = c_1^p \pmod q \in \mu_n(\mathbf{F}_q) \quad \text{et} \quad v = c_2^p \pmod q \in \mu_n(\mathbf{F}_q).$$

On a alors :

$$5(\overline{a}+\overline{b}) = 3u \quad \text{et} \quad \phi(\overline{a},\overline{b}) = 5v.$$

En posant

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^4},$$

on obtient :

$$5(\overline{a}'+\overline{b}') = 3 \quad \text{et} \quad \phi(\overline{a}',\overline{b}') = 5\zeta. \tag{1.27}$$

On en déduit que $\overline{b}'$ est racine du polynôme

$$P_{1,\zeta}(X) = X^4 - \frac{6}{5}X^3 + \frac{18}{25}X^2 - \frac{27}{125}X + \frac{81}{3125} - \zeta \in \mathbf{F}_q[X].$$

Avec les notations de la partie 1.1, l'égalité $P_{1,\zeta}(\overline{b}') = 0$ entraîne alors

$$\zeta \in \widetilde{A}(n,q).$$

Choisissons $\alpha_{1,\zeta}$ une racine carrée de $-225 + 10\delta_{1,\zeta}$ et $\beta_{1,\zeta}$ une racine carrée de $-225 - 10\delta_{1,\zeta}$ dans une clôture algébrique $\overline{\mathbf{F}_q}$ de $\mathbf{F}_q$. Les racines de $P_{1,\zeta}$ dans $\overline{\mathbf{F}_q}$ sont :

$$\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{1,\zeta}$ ou $\beta_{1,\zeta}$ est dans $\mathbf{F}_q$ et que $\zeta \in A(n,q)$. Par ailleurs, on a (formule (1.27))

$$\overline{a}' = \frac{3}{5} - \overline{b}'.$$

D'où :

$$\{\overline{a}',\overline{b}'\} = \left\{\frac{3}{10}+\frac{\alpha_{1,\zeta}}{50}, \frac{3}{10}-\frac{\alpha_{1,\zeta}}{50}\right\} \quad \text{ou} \quad \{\overline{a}',\overline{b}'\} = \left\{\frac{3}{10}+\frac{\beta_{1,\zeta}}{50}, \frac{3}{10}-\frac{\beta_{1,\zeta}}{50}\right\}.$$

On a donc respectivement

$$\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{1,\zeta}}{125} \quad \text{ou} \quad \overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{1,\zeta}}{125}.$$

Explicitons à présent l'équation de la courbe sur $\mathbf{F}_q$ déduite de (1.6) par réduction modulo q. Compte tenu de ce qui précède, il s'agit de l'équation

$$y^2 = x^3 - 5u^2(\overline{a}'^2 + \overline{b}'^2)x^2 + 5u^4\phi(\overline{a}',\overline{b}')x$$

qui est isomorphe sur $\mathbf{F}_q$ à la courbe d'équation

$$y^2 = x^3 - 5(\overline{a}'^2 + \overline{b}'^2)x^2 + 5\phi(\overline{a}', \overline{b}')x. \tag{1.28}$$

Si $\overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{1,\zeta}}{125}$, il s'agit de la courbe la courbe $F_{1,\zeta}$ d'équation

$$y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{1.29}$$

Si $\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{1,\zeta}}{125}$, il s'agit de la tordue quadratique de $F_{1,\zeta}$ par $\sqrt{-1}$, notée $F'_{1,\zeta}$. Elle a pour équation

$$y^2 = x^3 - \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{1.30}$$

Posons alors

$$a'_q(\zeta) = q + 1 - n'_{1,q}(\zeta) \tag{1.31}$$

où $n'_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbf{F}_q$ de $F'_{1,\zeta}$. On a

$$a'_q(\zeta) = \pm a_q(\zeta).$$

Il en résulte l'égalité

$$a_q(E)^2 = a_q(\zeta)^2. \tag{1.32}$$

D'après la congruence (1.16) et l'égalité (1.26), on en déduit que :

$$a_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p}.$$

C'est en contradiction avec la condition $1(c)$ du théorème 1.5.

2. Supposons que 5 ne divise pas $a+b$. Comme ci-dessus, il existe alors c_1 et c_2 deux entiers tels que :

$$a + b = 3c_1^p, \quad \phi(a,b) = c_2^p \quad \text{et} \quad c = c_1c_2.$$

D'après le lemme 1.25, q ne divise pas c, ainsi :

$$u = c_1^p \pmod{q} \in \mu_n(\mathbf{F}_q) \quad \text{et} \quad v = c_2^p \pmod{q} \in \mu_n(\mathbf{F}_q).$$

On a alors :

$$\overline{a} + \overline{b} = 3u \quad \text{et} \quad \phi(\overline{a}, \overline{b}) = v.$$

En posant

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^4},$$

on obtient :

$$\overline{a}' + \overline{b}' = 3 \quad \text{et} \quad \phi(\overline{a}', \overline{b}') = \zeta. \tag{1.33}$$

On en déduit que $\overline{b}'$ est racine du polynôme

$$P_{2,\zeta}(X) = X^4 - 6X^3 + 18X^2 - 27X + \frac{81 - \zeta}{5} \in \mathbf{F}_q[X].$$

Avec les notations de la partie 1.1, l'égalité $P_{2,\zeta}(\overline{b}') = 0$ entraîne alors

$$\zeta \in \widetilde{B}(n,q).$$

Choisissons $\alpha_{2,\zeta}$ une racine carrée de $-225+10\delta_{2,\zeta}$ et $\beta_{2,\zeta}$ une racine carrée de $-225-10\delta_{2,\zeta}$ dans $\overline{\mathbf{F}_q}$. Les racines de $P_{2,\zeta}$ dans $\overline{\mathbf{F}_q}$ sont alors :

$$\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10},\quad \frac{3}{2}-\frac{\alpha_{2,\zeta}}{10},\quad \frac{3}{2}+\frac{\beta_{2,\zeta}}{10},\quad \frac{3}{2}-\frac{\beta_{2,\zeta}}{10}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{2,\zeta}$ ou $\beta_{2,\zeta}$ est dans $\mathbf{F}_q$ et que $\zeta \in B(n,q)$. Par ailleurs, on a (formule (1.33))

$$\overline{a}' = 3-\overline{b}'.$$

D'où :

$$\{\overline{a}',\overline{b}'\}=\left\{\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10},\frac{3}{2}-\frac{\alpha_{2,\zeta}}{10}\right\}\quad\text{ou}\quad\{\overline{a}',\overline{b}'\}=\left\{\frac{3}{2}+\frac{\beta_{2,\zeta}}{10},\frac{3}{2}-\frac{\beta_{2,\zeta}}{10}\right\}.$$

On a donc respectivement

$$\overline{a}'^2+\overline{b}'^2=\frac{\delta_{2,\zeta}}{5}\quad\text{ou}\quad\overline{a}'^2+\overline{b}'^2=-\frac{\delta_{2,\zeta}}{5}.$$

Explicitons à présent l'équation de la courbe sur $\mathbf{F}_q$ déduite de (1.6) par réduction modulo q. Il s'agit de l'équation

$$y^2=x^3-5u^2(\overline{a}'^2+\overline{b}'^2)x^2+5u^4\phi(\overline{a}',\overline{b}')x$$

qui est isomorphe sur $\mathbf{F}_q$ à la courbe d'équation

$$y^2=x^3-5(\overline{a}'^2+\overline{b}'^2)x^2+5\phi(\overline{a}',\overline{b}')x.$$

Si $\overline{a}'^2+\overline{b}'^2=\frac{\delta_{2,\zeta}}{5}$, il s'agit de la courbe $F_{2,\zeta}$ d'équation

$$y^2=x^3+\delta_{2,\zeta}x^2+5\zeta x. \tag{1.34}$$

Si $\overline{a}'^2+\overline{b}'^2=-\frac{\delta_{2,\zeta}}{5}$, il s'agit de la tordue quadratique de $F_{2,\zeta}$ par $\sqrt{-1}$, notée $F'_{2,\zeta}$. Elle a pour équation

$$y^2=x^3-\delta_{2,\zeta}x^2+5\zeta x. \tag{1.35}$$

Posons alors comme ci-dessus

$$b'_q(\zeta)=q+1-n'_{2,q}(\zeta) \tag{1.36}$$

où $n'_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbf{F}_q$ de $F'_{2,\zeta}$. On a, à nouveau

$$b'_q(\zeta)=\pm b_q(\zeta),$$

puis

$$a_q(E)^2=b_q(\zeta)^2. \tag{1.37}$$

D'après la congruence (1.16) et l'égalité (1.26), on en déduit que :

$$b_q(\zeta)^2\equiv a_q(F)^2\pmod p,$$

ce qui contredit la condition $2(c)$ du théorème 1.5.

On aboutit ainsi à une contradiction à l'existence de $(a,b,c)\in S_p(3)$. Par suite, $S_p(3)$ est vide. Cela termine la démonstration du théorème 1.5.

1.4.5 Démonstration de la proposition 1.6

Il s'agit de montrer que l'équation $x^5+y^5=3z^p$ n'admet pas de solution propre et non triviale pour $5\leq p\leq 10^6$. C'est connu pour $p=5$ (cf. [Dir28]).

L'équation $x^5+y^5=3z^7$. On suppose que l'on a $p=7$. Pour toute courbe elliptique A de $\mathcal{F}_1$ et $\mathcal{F}_2$, il s'agit de montrer que ρ_7^E n'est pas isomorphe à ρ_7^A (lemme 1.24). Pour certaines de ces courbes A, on utilise pour cela la remarque suivante qui est une conséquance directe de la démonstration du théorème 1.5.

Remarque. Soit A l'une des courbes elliptiques de $\mathcal{F}_1$ (resp. de $\mathcal{F}_2$). Soit F l'unique courbe de $\mathcal{E}_1$ (resp. de $\mathcal{E}_2$) ayant le même invariant modulaire que A. Si l'on démontre l'existence d'un entier $n\geq 2$ pour lequel la condition 1 (resp. la condition 2) du théorème 1.5 est satisfaite, alors les représentations ρ_7^E et ρ_7^A ne sont pas isomorphes.

En utilisant cette remarque, on parvient à éliminer directement les courbes suivantes :

$$150\text{A1}, 150\text{B1}, 150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{E1},$$
$$1200\text{G1}, 1200\text{P1}, 1200\text{M1}, 1200\text{N1}, 1200\text{Q1}, 1200\text{S1}.$$

En effet, si $A\in\{150\text{C1}, 1200\text{P1}\}$, le couple $(F,n)=(150\text{C1},16)$ vérifie la condition 1 du théorème 1.5. On en déduit, comme au paragraphe précédent, que ρ_7^E et ρ_7^A ne sont pas isomorphes. De même :

- si $A\in\{600\text{A1}, 1200\text{E1}\}$, le couple $(F,n)=(600\text{A1},16)$ vérifie la condition 1 du théorème.
- Si $A\in\{600\text{F1}, 1200\text{G1}\}$, le couple $(F,n)=(600\text{F1},16)$ vérifie la condition 1 du théorème.
- Si $A\in\{150\text{A1}, 150\text{B1}, 1200\text{M1}, 1200\text{Q1}\}$, le couple $(F,n)=(150\text{A1},4)$ vérifie la condition 2 du théorème.
- Si $A\in\{1200\text{N1}, 1200\text{S1}\}$, le couple $(F,n)=(1200\text{N1},6)$ vérifie la condition 2 du théorème.

Il reste à montrer que ρ_7^E n'est pas isomorphe à ρ_7^A où A est l'une des courbes

$$1200\text{J1},\ 600\text{C1},\ 600\text{H1},\ 1200\text{B1 et } 1200\text{I1}.$$

Supposons que ρ_7^E soit isomorphe à ρ_7^A où $A=1200\text{J1}$. D'après le lemme 1.25, E a bonne réduction en $q=43$ car

$$a_q(1200\text{J1})=4\not\equiv\pm 2 \pmod 7. \tag{1.38}$$

De plus, d'après le lemme 1.24, 5 divise $a+b$. Déterminons les équations possibles de la courbe de Frey réduite modulo 43. On a

$$\mu_6(\mathbf{F}_{43})=\{1 \pmod{43}, 6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43},$$
$$37 \pmod{43}, 42 \pmod{43}\},$$

puis

$$\widetilde{A}(6,43)=\{6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43},$$
$$37 \pmod{43}, 42 \pmod{43}\}$$

et

$$A(6,43) = \{6 \pmod{43}, 7 \pmod{43}\}.$$

Avec les notations du paragraphe précédent, on a donc $\zeta = 6 \pmod{43}$ ou $\zeta = 7 \pmod{43}$.

Supposons que $\zeta = 6 \pmod{43}$. Alors, toujours avec les notations du paragraphe précédent, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,6}(X) &= X^4 + 16X^3 - X^2 - 4X + 22 \\ &= (X+2)(X+6)(X^2+8X+9) \in \mathbf{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = -2 \pmod{43}$ ou $-6 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (37 \pmod{43}, -2 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (41 \pmod{43}, -6 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbf{F}_{43}$ à la courbe $F'_{1,6}$ d'équation (cf. (1.28) et (1.30))

$$y^2 = x^3 - 28x^2 + 21x. \tag{1.39}$$

Supposons que $\zeta = 7 \pmod{43}$. Alors, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,7}(X) &= X^4 + 16X^3 - X^2 - 4X + 21 \\ &= (X+23)(X+28)(X^2+8X+22) \in \mathbf{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = 20 \pmod{43}$ ou $15 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (15 \pmod{43}, 20 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (20 \pmod{43}, 15 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbf{F}_{43}$ à la courbe $F_{1,7}$ d'équation (cf. (1.28) et (1.29))

$$y^2 = x^3 + 14x^2 + 3x. \tag{1.40}$$

Il en résulte que (1.39) et (1.40) sont les deux seules équations possibles pour la réduite de la courbe de Frey modulo 43. En particulier, on a $a_q(E) = a'_q(6) = -8$ ou $a_q(E) = a_q(7) = 10$ (cf (1.3) et (1.31)). D'après l'égalité (1.38) ci-dessus et la congruence (1.16), on a donc :

$$4 \equiv -8 \pmod{7} \quad \text{ou} \quad 4 \equiv 10 \pmod{7}.$$

On en déduit une contradiction. Les représentations ρ_7^E et ρ_7^A où $A = 1200\text{J}1$ ne sont donc pas isomorphes.

On procède de même pour éliminer les isomorphismes entre ρ_7^E et ρ_7^A où $A = 600\text{C}1, 1200\text{B}1$ et $1200\text{I}1$. On explicite donc certains calculs sans répéter exhaustivement les raisonnements.

Supposons que ρ_7^E soit isomorphe à ρ_7^A où A est la courbe 1200B1 ou la courbe 1200I1. Posons $n = 10$ et $q = 71$. On a

$$a_{71}(1200\text{B1}) = a_{71}(1200\text{I1}) = 4.$$

Donc, d'après le lemme 1.25, la courbe E a bonne réduction en q. On vérifie qu'il y a quatre équations possibles pour la réduite de E modulo 71. Il s'agit des courbes suivantes (cf. (1.5) et (1.36) et les équations (1.34) et (1.35)) :

$$\begin{aligned}
F'_{2,5} : y^2 &= x^3 - 24x^2 + 25x \quad \text{et } b'_{71}(5) = 0,\\
F_{2,5} : y^2 &= x^3 + 24x^2 + 25x \quad \text{et } b_{71}(5) = 0,\\
F'_{2,57} : y^2 &= x^3 - 14x^2 + x \quad \text{et } b'_{71}(57) = -8,\\
F'_{2,70} : y^2 &= x^3 - 32x^2 + 66x \quad \text{et } b'_{71}(70) = -4.
\end{aligned}$$

Par ailleurs, on a les congruences

$$a_{71}(E) \equiv b'_{71}(5),\ b_{71}(5),\ b'_{71}(57) \text{ ou } b'_{71}(70) \pmod 7.$$

D'où il résulte

$$4 \equiv 0,\ 3 \text{ ou } 6 \pmod 7.$$

On en déduit une contradiction : les représentations ρ_7^E et ρ_7^A où $A = 1200\text{B1}$ ou 1200I1 ne sont pas isomorphes.

De même, les représentations ρ_7^E et ρ_7^A, où A est la courbe 600C1, ne sont pas isomorphes. D'après le lemme 1.25, la courbe E a bonne réduction en $q = 197$ car $a_{197}(600\text{C1}) = 6$. Comme par ailleurs 5 ne divise pas $a + b$, on a onze équations possibles pour la courbe E réduite modulo 197 (cf. équations (1.34) et (1.35)). De plus,

$$\begin{array}{llll}
b_{197}(104) = 4, & b'_{197}(113) = 14, & b_{197}(113) = 14, & b'_{197}(120) = 10,\\
b_{197}(120) = 10, & b'_{197}(178) = -12, & b_{197}(196) = 8, & b'_{197}(77) = -18,\\
b_{197}(77) = -18, & b'_{197}(87) = 2, & b'_{197}(87) = 2. &
\end{array}$$

On conclut comme ci-dessus que les représentations ρ_7^E et ρ_7^A, où $A = 600\text{C1}$ ne sont pas isomorphes.

En revanche, pour la courbe $A = 600\text{H1}$ il n'existe aucun entier n tel que $6 < n < 1000$ pour lequel la méthode ci-dessus s'applique. Elle s'applique cependant avec $n = 6$, pourvu que l'on sache montrer que E a bonne réduction en $q = 43$, ce que le lemme 1.24 ne nous permet pas d'affirmer car

$$a_{43}(600\text{H1}) = -12 \equiv 2 \pmod 7.$$

Pour montrer que E a bonne réduction en 43, on utilise alors le résultat suivant.

Lemme 1.26 *Soient q un nombre premier et A une courbe elliptique sur $\mathbf{Q}$ ayant bonne réduction en q. Supposons que ρ_7^E soit isomorphe à ρ_7^A et que q vérifie les deux conditions suivantes :*

1. *on a $q \equiv 1 \pmod 7$ et $q \not\equiv 1 \pmod 5$.*

2. On a

$$a_q(A) \not\equiv 2\left(\frac{5}{q}\right) \pmod 7,$$

où $\left(\frac{5}{q}\right)$ *est le symbole de Legendre.*

Alors, E a bonne réduction en q.

Démonstration. Supposons que E ait mauvaise réduction en q. Puisque l'on a $q \neq 2, 5$, la courbe E a réduction de type multiplicatif en q (lemme 1.13). On a donc :

$$a_q(E) = \left(\frac{-c_6}{q}\right).$$

L'hypothèse $q \not\equiv 1 \pmod 5$ entraîne que q divise $a+b$ (lemme 1.12). Par suite, on a :

$$-c_6 = 2^6 \cdot 5^3 a^6 \pmod q,$$

d'où l'on déduit que l'on a

$$\left(\frac{-c_6}{q}\right) = \left(\frac{5}{q}\right).$$

Les représentations ρ_7^E et ρ_7^A étant isomorphes et A ayant bonne réduction en q, on a ([KO92, prop.3(iii)]) :

$$a_q(E)a_q(A) \equiv q+1 \pmod 7,$$

et compte tenu de la congruence $q \equiv 1 \pmod 7$, on obtient

$$a_q(E)a_q(A) \equiv 2 \pmod 7.$$

On a donc

$$a_q(A) \equiv 2\left(\frac{5}{q}\right) \pmod 7,$$

ce qui contredit la condition 2. D'où le lemme.

Déduisons-en que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes. Supposons le contraire. La courbe E a bonne réduction en $q = 43$. En effet, on a

$$a_{43}(A) = -12 \equiv 2 \pmod 7. \tag{1.41}$$

Puisque $\left(\frac{5}{43}\right) = -1$, on a

$$2 \equiv a_{43}(A) \not\equiv 2\left(\frac{5}{43}\right) \pmod 7,$$

d'où l'assertion d'après le lemme 1.26.

Par ailleurs, avec les notations de la partie 1.1, on a $B(6,43) = \{42 \pmod{43}\}$ et l'on vérifie que l'on a une seule courbe possible pour la réduction de E modulo 43. Elle a pour équation (cf. (1.35)) :

$$F'_{2,42} : y^2 = x^3 - 16x^2 + 38x.$$

On en déduit avec les formules (1.16), (1.36) et (1.41) que l'on a

$$2 \equiv a_{43}(A) \equiv b'_{43}(42) \equiv -1 \pmod 7.$$

On obtient ainsi une contradiction et le fait que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes.

Remarque. La même démonstration (appliquée à nouveau à $q = 43$) permettrait de redémontrer que les représentations ρ_7^E et ρ_7^A où $A = 1200\text{I}1$ ne sont pas isomorphes.

On a donc montré que $S_7(3)$ est vide.

L'équation $x^5 + y^5 = 3z^p$, pour $p \geq 11$. Pour $p \geq 11$, on utilise le critère énoncé dans le théorème 1.5 et le programme `Fermat` disponible à l'adresse `www.math.jussieu.fr/~billerey`.

Pour tout nombre premier p tel que $11 \leq p \leq 10^6$, et pour toute courbe elliptique F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, on trouve un entier $n \geq 2$ tel que le couple (F, n) vérifie la condition 1 du théorème 1.5 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

On obtient ainsi la proposition 1.6.

Remarque. On a indiqué dans le tableau 1.1 de l'Appendice A, les premières valeurs d' entiers n trouvés pour chaque courbe elliptique de $\mathcal{E}_\infty$ et $\mathcal{E}_\in$.

1.5 Annexe A – Tableau de valeurs

On a vu au §1.4.4 que si $q = np+1$ est un nombre premier congru à 1 modulo p et si E a bonne réduction en q, on est dans l'un des cas suivants (cf. (1.32) et (1.37)) :

1. il existe un élément $\zeta \in A(n, q)$ tel que
$$a_q(E) \equiv \pm a_q(\zeta) \pmod{p}.$$
2. Il existe un élément $\zeta \in B(n, q)$ tel que
$$a_q(E) \equiv \pm b_q(\zeta) \pmod{p}.$$

Il en résulte qu'il existe au plus $4n$ valeurs possibles pour la classe de $a_q(E)$ modulo p car les ensembles $A(n, q)$ et $B(n, q)$ sont de cardinal $\leq n$. Plus p est grand et n petit et plus la *probabilité* (en un sens heuristique) qu'une congruence de la forme
$$a_q(E)^2 \equiv a_q(F)^2 \pmod{p},$$
où F est l'une des courbes elliptiques des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, soit réalisée, est faible.

Cela porte à croire que, pour une courbe F des ensembles $\mathcal{E}_1$ ou $\mathcal{E}_2$ donnée, l'existence d'un entier n satisfaisant aux conditions du théorème 1.5 est d'autant plus probable que p est grand. De plus, on constate que pour les petites valeurs de p, on est souvent obligé de choisir une valeur de n pour chaque courbe elliptique, ce qui est « rarement » nécessaire lorsque p est grand (disons $p > 10000$).

Dans le tableau 1.1, on a on a indiqué dans la première colonne la liste des nombres premiers p compris entre 11 et 150. Les courbes elliptiques inscrites sur la première ligne sont celles des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$. Pour un nombre premier p et une courbe elliptique F comme ci-dessus, on lit dans la case correspondante

un entier n tel que le couple (F, n) vérifie la condition 1 du théorème 1.5 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

Ces valeurs ont été obtenues à l'aide du programme `Fermat` disponible à l'adresse `www.math.jussieu.fr/~billerey`.

	150C1	600A1	600F1	1200J1	150A1	600C1	1200N1
11	2	2	2	2	2	2	2
13	4	4	4	4	6	4	4
17	6	6	6	6	14	8	14
19	10	24	24	10	22	22	12
23	2	2	2	2	2	2	2
29	2	2	2	2	2	2	2
31	10	10	22	22	10	10	42
37	4	4	4	4	4	4	6
41	2	2	2	2	2	2	2
43	4	4	4	4	10	4	4
47	6	6	6	6	6	6	6
53	2	2	2	2	2	2	2
59	12	18	18	12	12	18	12
61	12	6	12	6	12	6	6
67	4	4	4	4	4	4	4
71	8	8	8	8	8	8	8
73	4	4	6	4	4	4	6
79	4	4	18	18	18	4	4
83	2	2	2	2	2	2	2
97	4	4	4	4	4	4	4
101	8	6	6	6	8	36	6
103	6	12	10	12	10	10	6
107	6	6	6	6	6	6	6
109	30	10	10	10	10	10	10
113	14	2	14	2	2	2	2
127	4	18	4	4	4	4	4
131	2	2	8	2	2	2	2
137	6	6	6	6	6	6	6
139	4	4	4	4	4	4	4
149	8	8	8	8	8	8	8

TAB. 1.1 – Tableau des premières valeurs d'entiers n vérifiant les conditions du théorème 1.5.

1.6 Annexe B – Courbes de conducteur 150, 600 et 1200

Les notations du tableau 1.2 sont celles des tables de [Cre97]. Pour un représentant F de chaque classe d'isogénie de courbes de conducteur 150, 600 ou 1200, on donne successivement :

- un quintuplet $[a_1, a_2, a_3, a_4, a_6]$ tel que

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

  soit une équation minimale de Weierstrass de F,
- l'invariant modulaire j_F de F,
- la valuation en 5, $v_5(j_F)$, de l'invariant modulaire j_F de F,
- la valuation en 5, $v_5(\Delta_m(F))$, du discriminant minimal de F,
- l'indice de ramification e en 5 de l'extension $\mathbf{Q}(F[p])/\mathbf{Q}$ engendrée par les coordonnées des points de p-torsion de la courbe F. Si $v_5(j_F) \geq 0$, c'est le dénominateur de $v_5(\Delta_m(F))/12$ et si $v_5(j_F) < 0$, compte tenu du fait que p ne divise pas $v_5(j_F)$, on a $e = 2p$ (cf. [CK02]).

courbe	équation	j_F	$v_5(j_F)$	$v_5(\Delta_m(F))$	e
150A1	$[1,0,0,-3,-3]$	$-24389/12$	0	3	4
150B1	$[1,1,0,-75,-375]$	$-24389/12$	0	9	4
150C1	$[1,1,1,37,281]$	$357911/2160$	-1	7	$2p$
600A1	$[0,-1,0,-383,3012]$	$24918016/45$	-1	7	$2p$
600B1	$[0,-1,0,7,-3]$	$5120/3$	1	2	6
600C1	$[0,-1,0,32,-68]$	$27436/27$	0	3	4
600D1	$[0,1,0,17,38]$	$2048/3$	0	6	2
600E1	$[0,1,0,-233,1563]$	$-8780800/2187$	2	4	3
600F1	$[0,-1,0,92,-188]$	$21296/15$	-1	7	$2p$
600G1	$[0,-1,0,-5833,207037]$	$-8780800/2187$	2	10	6
600H1	$[0,1,0,792,-6912]$	$27436/27$	0	9	4
600I1	$[0,1,0,167,-37]$	$5120/3$	1	8	3
1200A1	$[0,-1,0,17,-38]$	$2048/3$	0	6	2
1200B1	$[0,-1,0,792,6912]$	$27436/27$	0	9	4
1200C1	$[0,-1,0,167,37]$	$5120/3$	1	8	3
1200D1	$[0,-1,0,-233,-1563]$	$-8780800/2187$	2	4	3
1200E1	$[0,1,0,-383,-3012]$	$24918016/45$	-1	7	$2p$
1200F1	$[0,1,0,7,3]$	$5120/3$	1	2	6
1200G1	$[0,1,0,92,188]$	$21296/15$	-1	7	$2p$
1200H1	$[0,1,0,-5833,-207037]$	$-8780800/2187$	2	10	6
1200I1	$[0,1,0,32,68]$	$27436/27$	0	3	4
1200J1	$[0,-1,0,-8,-1488]$	$-1/15$	-1	7	$2p$
1200K1	$[0,-1,0,27,-243]$	$20480/243$	1	2	6
1200L1	$[0,-1,0,-333,3537]$	$-40960/27$	1	8	3
1200M1	$[0,-1,0,-48,192]$	$-24389/12$	0	3	4
1200N1	$[0,-1,0,-333,-2088]$	$131072/9$	0	9	4
1200O1	$[0,1,0,-13,23]$	$-40960/27$	1	2	6
1200P1	$[0,1,0,592,-16812]$	$357911/2160$	-1	7	$2p$
1200Q1	$[0,1,0,-1208,21588]$	$-24389/12$	0	9	4
1200R1	$[0,1,0,-133,563]$	$-102400/3$	2	4	3
1200S1	$[0,1,0,-13,-22]$	$131072/9$	0	3	4

TAB. 1.2 – Classes d'isogénie des courbes elliptiques de conducteur 150, 600 et 1200

Chapitre 2

Formes homogènes de degré 3 et puissances p-ièmes

Ce chapitre correspond à l'article [Bil08a] paru au Journal of Number Theory *à l'exception des modifications suivantes :*

- *ajout de la remarque, de la note de bas de page et de références dans l'introduction ;*
- *ajout du §2.4.1 ;*
- *modification de la démonstration de 2.36 pour rendre le résultat effectif.*

Introduction

On se propose de faire quelques remarques sur la conjecture suivante.

Conjecture 2.1 (A) *Soient $F \in \mathbf{Z}[X,Y]$ une forme homogène séparable de degré ≥ 3 et d un entier ≥ 1. Il existe une constante $C_{d,F} > 0$ ne dépendant que de d et F telle que si p est un nombre premier $> C_{d,F}$ et (a,b,c) un triplet d'entiers non nuls premiers entre eux vérifiant l'égalité*

$$F(a,b) = dc^p,$$

alors on a $c = \pm 1$.

Remarque. Lorsque $F(X,Y) = XY(X+Y)$, l'énoncé de la conjecture ci-dessus correspond au théorème de Fermat.

Hormis le cas du théorème de Fermat, les seuls résultats déjà connus sur cette conjecture concernent certains cas particuliers d'équations de Fermat généralisées où d est un entier convenablement choisi et où $F(x,y)$ est l'une des formes suivantes (cf. [Kra98, CS09, Ell04, Die05a, Die05b, Dar93, Bil07, BD08, Kra02]) :

$$x^3+y^3, \quad x^4+y^4, \quad x^4-y^4, \quad x^5+y^5 \quad \text{et} \quad x^6+y^6.$$

Les équations $F(x,y) = \pm d$ d'inconnues x, y dans $\mathbf{Z}$ sont appelées équations de Thue. Elles ont été particulièrement étudiées. On sait par exemple qu'elles n'ont qu'un nombre fini de solutions (cf. par exemple [HS00, p.363]). Par ailleurs, si $p \geq 5$ est fixé, un théorème de [DG95] affirme qu'il n'existe qu'un nombre fini

de triplets d'entiers non nuls (a, b, c) premiers entre eux tels que $F(a, b) = dc^p$. La conjecture (A) entraîne donc que l'ensemble des triplets (a, b, c) d'entiers non nuls premiers entre eux pour lesquels il existe un nombre premier $p \geq 5$ tel que $F(a, b) = dc^p$, est fini.

On rappelle dans l'Appendice 2.4 que la conjecture (A) est une conséquence de la conjecture *abc*.

Dans cet article, on s'intéresse plus spécifiquement aux équations diophantiennes de la forme

$$F(x, y) = dz^p, \tag{2.1}$$

où F est une forme homogène séparable de degré 3 à coefficients entiers relatifs, p un nombre premier ≥ 7 et d un entier ≥ 1.

Le cas particulier de l'équation (2.1)

$$x^3 + y^3 = z^p, \tag{2.2}$$

a été étudié[1] par H. Darmon et A. Granville ([DG95]) et A. Kraus ([Kra98]). Leur approche repose sur l'étude modulaire de la représentation galoisienne des points de p-torsion d'une certaine courbe elliptique, appelée parfois courbe de Frey ou courbe de Hellegouarch-Frey, associée à une hypothétique solution de l'équation (2.2).

Conformément à la terminologie utilisée dans [DG95], on dira qu'un triplet d'entiers $(a, b, c) \in \mathbf{Z}^3$ est solution de l'équation (2.1) si $F(a, b) = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Dans la partie 2.1, on généralise la construction de la courbe de Frey associée à l'équation (2.2) dans [DG95] à toutes les formes homogènes séparables de degré 3

$$F(x, y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3,$$

avec t_0, t_1, t_2 et t_3 entiers relatifs. Si (a, b, c) est une solution propre et non triviale de (2.1), la courbe E que l'on construit a pour équation

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 &= t_1a - t_2b, \\ a_4 &= t_0t_2a^2 + (3t_0t_3 - t_1t_2)ab + t_1t_3b^2, \\ a_6 &= t_0^2t_3a^3 - t_0(t_2^2 - 2t_1t_3)a^2b + t_3(t_1^2 - 2t_0t_2)ab^2 - t_0t_3^2b^3. \end{cases}$$

On démontre au théorème 2.5 que si p est assez grand et $c \neq \pm 1$, alors E est une courbe de Frey au sens de la définition 2.4.

Cette construction offre l'avantage de relier le problème diophantien soulevé par l'équation (2.1) à des résultats ou conjectures classiques de théorie des nombres ou, plus spécifiquement, de la théorie des courbes elliptiques. Tel est le cas, par exemple, de la conjecture suivante, attribuée à G. Frey et B. Mazur (cf. [Dar95] et [Kra99]) :

[1] Récemment, Chen et Siksek ([CS09]) ont montré que l'équation (2.2) n'admet aucune solution propre et non triviale pour un ensemble de nombres premiers p de densité ≈ 0.628. Leur approche combine la méthode modulaire à des résultats sur les obstructions (de type Brauer-Manin) à l'existence de points rationnels sur certaines équations hyperelliptiques.

Conjecture 2.2 (Frey-Mazur) *Soit A une courbe elliptique définie sur $\mathbf{Q}$. On désigne par $\mathcal{F}_A$ l'ensemble des nombres premiers ℓ pour lesquels il existe une courbe elliptique $A^{(\ell)}$ définie sur $\mathbf{Q}$, non isogène à A sur $\mathbf{Q}$, telle que les modules galoisiens des points de ℓ-torsion de A et $A^{(\ell)}$ soient isomorphes. Alors, l'ensemble $\mathcal{F}_A$ est fini.*

Cette conjecture n'a actuellement été démontrée pour aucune courbe elliptique. Si A est une courbe elliptique définie sur $\mathbf{Q}$, on sait que 2, 3 et 5 sont dans $\mathcal{F}_A$.

En utilisant la construction de E, on montre (proposition 2.11) que la conjecture ci-dessus implique la conjecture (A) pour les formes homogènes de degré 3.

On donne par ailleurs dans l'Appendice 2.5 une démonstration, due à Kraus, du fait que la conjecture *abc* implique (via une forme faible de la conjecture de Szpiro) la conjecture de Frey-Mazur. On a donc en résumé le diagramme d'implications suivant.

$$\begin{array}{ccc} \text{Conjecture de Frey-Mazur} & \Longleftarrow\!\!= & \text{Conjecture } abc \\ \Downarrow & & \Downarrow \\ \text{Conjecture } (A) \text{ pour } \deg(F) = 3 & & \text{Conjecture } (A) \end{array}$$

Si F est une forme homogène séparable de degré ≥ 3 à coefficients entiers relatifs, on pose $f(x) = F(x, 1)$. Lorsque $d = 1$ et $y = 1$, l'équation (2.1) s'écrit

$$f(x) = z^p. \tag{2.3}$$

En 1920, Nagell a démontré que pour le polynôme

$$f(x) = x^3 + x^2 + x + 1, \tag{2.4}$$

l'équation (2.3) n'admettait pas de solution non triviale ($xz \neq 0$) pour $p \geq 3$ et seulement $(x, z) = (7, 20)$ lorsque $p = 2$ ([Nag02, p.73]). Outre le cas particulier de l'équation de Catalan, $x^3 \pm z^p = 1$, on trouvera d'autres exemples de résolution de telles équations dans [BVY04] et [BHM02].

Suivant l'exemple de Nagell, nous illustrons dans la partie 2.2 la construction de la courbe de Frey précédente avec l'étude de l'équation (2.1) lorsque F est la forme homogène de degré 3 suivante

$$F(x, y) = x^3 + x^2y + xy^2 + y^3. \tag{2.5}$$

Si (a, b, c) appartient à l'ensemble $S_p(d)$ des solutions propres et non triviales de l'équation (2.1) où F est la forme ci-dessus et d un entier ≥ 1, on lui associe la courbe E d'équation

$$E : y^2 = x^3 + (a - b)x^2 + (a + b)^2x + a^3 + a^2b - ab^2 - b^3.$$

Pour certains entiers d libres de puissances troisièmes, on obtient plusieurs résultats sur $S_p(d)$. À titre d'exemple, on montre par des arguments de nature modulaire (théorème 2.13) que si $d = 2$, 6, 10 ou 22, alors $S_p(d)$ est vide pour $p \geq 7$. De même, si ℓ est un nombre premier vérifiant certaines conditions explicites, alors $S_p(2\ell)$ est vide lorsque p est suffisamment grand. Tel est le cas, par exemple, lorsque $\ell = 19, 43, 59, 61, 67, 83$ (théorème 2.14).

Bien que notre construction ne permette pas de retrouver le résultat de Nagell (correspondant au cas où $d = 1$ et $y = 1$), on explique dans la partie 2.3 comment la théorie modulaire permet d'aborder, voire de résoudre complètement, certaines équations diophantiennes, certes plus artificielles mais néanmoins non triviales, de la forme (2.1) ou (2.3) lorsque le polynôme considéré est de degré ≥ 3.

2.1 La courbe elliptique E

On considère dans cette partie une forme homogène séparable de degré 3 à coefficients entiers relatifs

$$F(x, y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3.$$

Posons $f(x) = F(x, 1)$. Le polynôme F étant séparable, il en va de même pour f.

On considère un nombre premier $p \geq 7$, un entier $d \geq 1$ et (a, b, c) une solution propre et non triviale de l'équation (2.1).

2.1.1 Équation de la courbe E

On commence par supposer $t_0 \neq 0$, i.e. $\deg(f) = 3$. Soit $K = \mathbf{Q}(\alpha, \beta, \gamma)$ l'extension de $\mathbf{Q}$ dans $\mathbf{C}$ engendrée par les racines α, β, γ du polynôme f. On a alors la factorisation suivante :

$$F(x, y) = t_0(x - \alpha y)(x - \beta y)(x - \gamma y).$$

On associe à (a, b, c) une courbe elliptique $E/\mathbf{Q}$ comme suit. Posons :

$$\left\{ \begin{array}{rcl} A & = & t_0(\beta - \gamma)(a - \alpha b), \\ B & = & t_0(\gamma - \alpha)(a - \beta b), \\ C & = & t_0(\alpha - \beta)(a - \gamma b). \end{array} \right.$$

Par construction, on a

$$A + B + C = 0.$$

Soit $\mathcal{E}$ la cubique d'équation :

$$\mathcal{E} : Y^2 = X(X - A)(X + B). \tag{2.6}$$

Son disciminant est

$$\Delta(\mathcal{E}) = 16(AB)^2(A + B)^2 = 16\mathfrak{D}(f)F(a, b)^2,$$

où $\mathfrak{D}(f)$ est le discriminant du polynôme f. L'entier c étant non nul et le polynôme f séparable, on a $\Delta(\mathcal{E}) \neq 0$. L'équation (2.6) définit donc une courbe elliptique sur K.

Considérons les trois éléments u_1, u_2 et u_3 de K définis par

$$\left\{ \begin{array}{rcl} u_1 & = & t_0(\alpha a + \gamma\beta b), \\ u_2 & = & t_0(\beta a + \gamma\alpha b), \\ u_3 & = & t_0(\gamma a + \beta\alpha b). \end{array} \right.$$

Ils vérifient les égalités : $A = u_2 - u_3$, $B = u_3 - u_1$ et $C = u_1 - u_2$. Le changement de variables

$$x = X + u_3, \quad y = Y, \tag{2.7}$$

transforme alors l'équation (2.6) en l'équation :

$$E : y^2 = (x - u_1)(x - u_2)(x - u_3).$$

Cette courbe E a pour équation :

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \tag{2.8}$$

avec

$$\begin{cases} a_2 &= t_1 a - t_2 b, \\ a_4 &= t_0 t_2 a^2 + (3t_0 t_3 - t_1 t_2)ab + t_1 t_3 b^2, \\ a_6 &= t_0^2 t_3 a^3 - t_0(t_2^2 - 2t_1 t_3)a^2 b + t_3(t_1^2 - 2t_0 t_2)ab^2 - t_0 t_3^2 b^3. \end{cases}$$

La courbe elliptique E est donc définie sur $\mathbf{Q}$ et le changement de variables (2.7) fournit un isomorphisme défini sur K de $\mathcal{E}$ sur E. De plus, les invariants standard $c_4(E)$ et $\Delta(E)$ de (2.8) sont inchangés par rapport à ceux de $\mathcal{E}$ (cf. [Tat75]). On les note respectivement c_4 et Δ. On a :

$$\begin{cases} c_4 &= 16\big((t_1^2 - 3t_0 t_2)a^2 + (t_1 t_2 - 9t_0 t_3)ab + (t_2^2 - 3t_1 t_3)b^2\big), \\ \Delta &= 16\mathfrak{D}(f)F(a,b)^2 \\ & \quad \text{où } \mathfrak{D}(f) = -27t_0^2 t_3^2 + (18t_1 t_2 t_3 - 4t_2^3)t_0 - 4t_3 t_1^3 + t_1^2 t_2^2. \end{cases} \tag{2.9}$$

Supposons $t_0 = 0$. Dans ce cas, on associe à (a, b, c) la courbe ellipitique $E/\mathbf{Q}$ d'équation

$$E : y^2 = x^3 + (t_1 a - t_2 b)x^2 + t_1(t_3 b - t_2 a)bx + t_1^2 t_3 ab^2.$$

Il s'agit de la courbe d'équation (2.8) avec $t_0 = 0$.

Remarque 2.3 *Supposons qu'il existe $x_0 \in \mathbf{Q}$ racine du polynôme f. Alors, E a un point d'ordre 2 rationnel sur $\mathbf{Q}$. Si $x_0 = 0$, tel est le cas du point $(t_2 b, 0)$, sinon tel est le cas de $(t_0 x_0 a - \frac{t_3}{x_0} b, 0)$.*

2.1.2 La courbe de Frey E

On rappelle que p est un nombre premier ≥ 7 et que (a, b, c) est une solution propre et non triviale de l'équation (2.1). Notons $\overline{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ le groupe de Galois absolu de $\mathbf{Q}$. Soit A une courbe elliptique définie sur $\mathbf{Q}$ et $A[p]$ le sous-groupe de $A(\overline{\mathbf{Q}})$ constitué des points de p-torsion de A. C'est un $\mathbf{F}_p$-espace vectoriel de dimension 2 sur lequel le groupe $\mathrm{G}_{\mathbf{Q}}$ opère continûment. Par le choix d'une base de $A[p]$ sur $\mathbf{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^A : \mathrm{G}_{\mathbf{Q}} \longrightarrow \mathbf{GL}_2(\mathbf{F}_p).$$

On associe à cette représentation un poids k qui est un entier ≥ 2 et un conducteur $N(\rho_p^A)$ qui est un entier ≥ 1, premier à p, qui divise le conducteur N_A de A (cf. [Ser87, §1]). Désignons par Δ_A le discriminant minimal de A. Si ℓ est un nombre premier, notons v_ℓ la valuation ℓ-adique de $\mathbf{Q}$.

Définition 2.4 *Soit $A/\mathbf{Q}$ une courbe elliptique définie sur $\mathbf{Q}$. On désigne par S_A l'ensemble des nombres premiers de mauvaise réduction de A. Soient S un sous-ensemble de S_A et p un nombre premier. On dira que A est une courbe de Frey associée au couple (p, S) si les trois conditions suivantes sont satisfaites.*

1. *La représentation ρ_p^A est irréductible.*
2. *L'ensemble S est strictement inclus dans S_A.*
3. *Pour tout nombre premier $\ell \in S_A \backslash S$, la courbe A a réduction multiplicative en ℓ et $v_\ell(\Delta_A) \equiv 0 \pmod{p}$.*

Avec la définition ci-dessus, on a le résultat suivant.

Théorème 2.5 *Il existe une constante $\alpha(d, F) \geq 0$ ne dépendant que de d et F telle que si $c \neq \pm 1$ et $p > \alpha(d, F)$, alors la courbe E est une courbe de Frey associée au couple (p, S) où S est l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ de mauvaise réduction.*

Démontrons à présent cet énoncé.

Résultats préliminaires

On a la relation suivante :

$$U(a,b)F(a,b) + V(a,b)c_4 = -16\mathfrak{D}(f)b^4, \tag{2.10}$$

où

$$\begin{cases} U(a,b) &= 16\Big(3t_0(3t_0t_2 - t_1^2)a + (t_1^3 - 6t_0t_1t_2 + 27t_0^2t_3)b\Big) \\ V(a,b) &= 3t_0^2a^2 + 2t_0t_1ab + (4t_0t_2 - t_1^2)b^2. \end{cases}$$

On en déduit le lemme suivant.

Lemme 2.6 *Soit ℓ un nombre premier divisant Δ et ne divisant pas $2d\mathfrak{D}(f)$. L'équation (2.8) est minimale en ℓ et la courbe E a réduction multiplicative en ℓ. De plus, $v_\ell(\Delta_E)$ est multiple de p.*

DÉMONSTRATION : Soit ℓ un nombre premier impair ne divisant pas $d\mathfrak{D}(f)$ et divisant $\Delta = 2^4\mathfrak{D}(f)d^2c^{2p}$. Nécessairement, ℓ divise l'entier c. Supposons par l'absurde que ℓ divise le coefficient c_4. D'après la relation (2.10), l'entier ℓ divise alors également $16\mathfrak{D}(f)b^4$. Or ℓ ne divise pas $2\mathfrak{D}(f)$, donc ℓ divise b. De l'expression de $F(a,b)$, on en déduit que ℓ divise t_0a^3. Si ℓ ne divise pas a, alors ℓ divise t_0 et d'après l'expression du coefficient c_4 de la courbe E ci-dessus, il vient que ℓ divise également t_1. Mais alors ℓ divise $\mathfrak{D}(f)$ d'après l'expression (2.9) ci-dessus. C'est une contradiction. Donc ℓ divise a. Comme ℓ divise aussi b et c, c'est contraire au fait que (a, b, c) soit une solution propre de (2.1). On en déduit que ℓ ne divise pas c_4.

La congruence $v_\ell(\Delta_E) \equiv 0 \pmod{p}$ résulte de l'égalité $v_\ell(\Delta) = v_\ell(\Delta_E)$ et de l'expression (2.9) du coefficient Δ.

Lemme 2.7 *Pour p assez grand, la représentation ρ_p^E est irréductible. Si E a un point d'ordre 2 rationnel sur $\mathbf{Q}$, c'est le cas pour $p \geq 11$. Si l'invariant modulaire j de E est différent de -15^3 et 255^3, la représentation ρ_7^E est irréductible.*

DÉMONSTRATION : La représentation ρ_p^E est irréductible dès que $p > 163$ d'après [Maz78].

Supposons que E a un point d'ordre 2 rationnel sur $\mathbf{Q}$ (c'est par exemple le cas si f est réductible sur $\mathbf{Q}$ d'après la remarque 2.3). Si ρ_p^E était réductible, le groupe $E(\overline{\mathbf{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $\mathrm{G}_{\mathbf{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbf{Q}$. Or, si $p \geq 11$, B. Mazur et M. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbf{Q})$ est vide (cf. [Ken82]). D'où le résultat dans ce cas.

Le cas $p = 7$ se traite en remarquant que la courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [Cre97] et qu'elle possède exactement deux points rationnels sur $\mathbf{Q}$ qui correspondent aux deux classes de $\overline{\mathbf{Q}}$-isomorphisme des courbes elliptiques d'invariants $j = -15^3$ et 255^3 ([Lig75, p.45]). D'où le lemme.

Lemme 2.8 *Si p ne divise pas $d\mathfrak{D}(f)$, alors on a $k = 2$.*

DÉMONSTRATION : On suppose que p ne divise pas $d\mathfrak{D}(f)$. Alors, d'après le lemme 2.6, l'équation (2.8) est minimale en p, la courbe E a réduction semi-stable en p et l'exposant de p dans le discriminant minimal de E est multiple de p. D'où $k = 2$ ([Ser87, prop. 5]).

Le lemme suivant servira à plusieurs reprises (pour un résultat plus précis, voir [Spr93, V.§4]).

Lemme 2.9 *Soit S' un ensemble fini de nombres premiers. Il n'existe qu'un nombre fini de triplets d'entiers (u, v, m) vérifiant les trois conditions suivantes :*

1. *on a $F(u, v) = m$,*
2. *les entiers u et v sont premiers entre eux,*
3. *l'entier m a tous ses diviseurs premiers dans S'.*

DÉMONSTRATION : Posons $S' = \{p_1, \ldots, p_r\}$. Soit $n \in \mathbf{Z} \setminus \{0\}$. L'ensemble

$$\left\{ (x, y) \in \mathbf{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x, y) = n \right\}$$

est fini ([HS00, p.363]).

On en déduit que si $\mathcal{N} = \{\pm p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ \text{avec } 0 \leq \alpha_i \leq 2\}$, alors l'ensemble

$$\mathcal{F} = \left\{ (x, y) \in \mathbf{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x, y) = n,\ \text{avec } n \in \mathcal{N} \right\}$$

est encore fini.

Soit (u, v, m) un triplet d'entiers vérifiant les trois conditions du lemme. Il existe un unique entier $Z > 0$ ayant tous ses diviseurs premiers dans S' tel que $m = Z^3 n$ avec $n \in \mathcal{N}$. On a alors

$$F\left(\frac{u}{Z}, \frac{v}{Z}\right) = n.$$

En particulier, il existe r et s tels que

$$\left(\frac{u}{Z}, \frac{v}{Z}\right) = (r, s) \in \mathcal{F}.$$

Les entiers u et v étant premiers entre eux, l'entier Z est le plus petit dénominateur commun > 0 de r et s. On en déduit qu'il n'existe qu'un nombre fini de valeurs possibles pour u et v et, par conséquent, pour m. Cela démontre le lemme.

Notations. Soit S' un ensemble fini non vide de nombres premiers. On désigne par $\mathcal{F}_{F,S'}$ l'ensemble (fini) des triplets (u,v,m) satisfaisant aux trois conditions du lemme 2.9. On pose alors

$$N_{F,S'} = \begin{cases} \max\{|m|, (u,v,m) \in \mathcal{F}_{F,S'}\} & \text{si } \mathcal{F}_{F,S'} \neq \emptyset \\ 1 & \text{sinon.} \end{cases} \tag{2.11}$$

L'entier $N_{F,S'}$ ne dépend que de F et S'.

Lemme 2.10 *Il existe une constante $\beta(d,F) \geq 0$ ne dépendant que de d et F telle que si $p > \beta(d,F)$, alors l'une des deux conditions suivantes est réalisée :*

1. *on a $c = \pm 1$,*
2. *il existe un nombre premier ne divisant pas $2d\mathfrak{D}(f)$ en lequel E a mauvaise réduction.*

DÉMONSTRATION : Supposons la seconde condition non réalisée. Alors, d'après le lemme 2.6, l'entier c a tous ses diviseurs premiers dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)$. Par ailleurs, si $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b, alors $(\mathrm{pgcd}(a,b))^3$ divise d. Posons

$$a' = \frac{a}{\mathrm{pgcd}(a,b)}, \quad b' = \frac{b}{\mathrm{pgcd}(a,b)} \quad \text{et} \quad d' = \frac{d}{(\mathrm{pgcd}(a,b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.9, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations précédentes)

$$\beta(d,F) = \frac{\log N_{F,S'}}{\log 2} \geq 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $\beta(d,F)$. Si l'on a $p > \beta(d,F)$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. Cela démontre le lemme 2.10.

Fin de la démonstration du théorème 2.5

Notons S l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ en lesquels la courbe E a mauvaise réduction. D'après le lemme 2.7, il existe une constante $\gamma(d,F) \geq 5$ telle que si $p > \gamma(d,F)$, alors ρ_p^E est irréductible. Posons, avec les notations du lemme 2.10, $\alpha(d,F) = \max(\beta(d,F), \gamma(d,F))$. Si $c \neq \pm 1$ et $p > \alpha(d,F)$, alors $p > \beta(d,F)$ et, d'après le lemme 2.10, il existe un nombre premier de mauvaise réduction qui ne soit pas dans S, i.e. $S_E \setminus S \neq \emptyset$. Par ailleurs, d'après le lemme 2.6, pour tout nombre premier $\ell \in S_E \setminus S$, E a réduction multiplicative en ℓ et $v_\ell(\Delta_E) \equiv 0 \pmod{p}$. D'où le théorème.

2.1.3 Lien avec la conjecture de Frey - Mazur

Notation. Soit A une courbe elliptique définie sur $\mathbf{Q}$. On pose, avec les notations de la conjecture de Frey-Mazur,

$$\nu_A = \max\{\ell \mid \ell \in \mathcal{F}_A\}.$$

D'après cette conjecture, $\nu_A \in \mathbf{N}$.

Proposition 2.11 *La conjecture de Frey-Mazur implique la conjecture (A) pour les formes de degré* 3.

DÉMONSTRATION : D'après les lemmes 2.7 et 2.8, on peut sans restriction supposer la représentation ρ_p^E irréductible et de poids 2. Le conducteur $N(\rho_p^E)$ est majoré par une constante M indépendante du quadruplet (a,b,c,p). En effet, si ℓ est un diviseur premier de $N(\rho_p^E)$, alors, d'après le lemme 2.6 et [Kra97a, p. 28], ℓ divise $2d\mathfrak{D}(f)$. De plus, on a $v_2(N(\rho_p^E)) \leq 8$, $v_3(N(\rho_p^E)) \leq 5$ et si $\ell \geq 5$, $v_\ell(N(\rho_p^E)) \leq 2$ (cf. [Pap93]). On peut donc, par exemple, choisir $M = (2d\mathfrak{D}(f))^8$.

Par ailleurs, d'après le théorème 3 de [Kra97b], il existe une constante $\eta_{d,F}$ ne dépendant que de d et F telle que si $p > \eta_{d,F}$, alors il existe une courbe elliptique A définie sur $\mathbf{Q}$ de conducteur $N_A = N(\rho_p^E)$ telle que les représentations ρ_p^E et ρ_p^A soient isomorphes.

Supposons l'inégalité suivante vérifiée

$$p > \nu_{d,F} = \max\{\eta_{d,F}, \nu_{A'} \mid A' \text{ courbe elliptique sur } \mathbf{Q} \text{ telle que } N_{A'} \leq M\}.$$

L'entier M ne dépendant que de d et F, il en va de même pour $\nu_{d,F}$. Considérons alors ℓ un nombre premier divisant c et ne divisant pas $2d\mathfrak{D}(f)N_A$. En particulier, ℓ divise Δ sans diviser $2d\mathfrak{D}(f)$, donc, d'après le lemme 2.6, la courbe E a mauvaise réduction multiplicative en ℓ. De plus, comme $p > \nu_{d,F} \geq \nu_A$, les courbes E et A sont $\mathbf{Q}$-isogènes d'après la conjecture de Frey-Mazur et on a

$$1 = v_\ell(N_E) = v_\ell(N_A) = 0, \quad \text{car } \ell \text{ ne divise pas } N_A.$$

C'est une contradiction. On en déduit que c a tous ses diviseurs premiers inclus dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)\prod N_{A'}$ où le produit porte sur l'ensemble fini (cf. [Sil92, IX §6]) des classes de $\mathbf{Q}$-isomorphisme de courbes elliptiques A' définies sur $\mathbf{Q}$ de conducteur $\leq M$.

Si $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b, alors $(\mathrm{pgcd}(a,b))^3$ divise d. Posons

$$a' = \frac{a}{\mathrm{pgcd}(a,b)}, \quad b' = \frac{b}{\mathrm{pgcd}(a,b)} \quad \text{et} \quad d' = \frac{d}{(\mathrm{pgcd}(a,b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.9, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations (2.11))

$$C_{d,F} = \frac{\log N_{F,S'}}{\log 2} \geq 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $C_{d,F}$. Et, si $p > C_{d,F}$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. C'est l'énoncé de la conjecture (A) .

2.2 Étude d'un exemple

À titre d'exemple, on applique, dans cette partie, la construction précédente au cas particulier de la forme homogène

$$F(x,y) = x^3 + x^2y + xy^2 + y^3.$$

Soient p un nombre premier ≥ 7 et d un entier ≥ 1. Rappelons que $S_p(d)$ désigne l'ensemble des solutions propres et non triviales de l'équation

$$F(x,y) = x^3 + x^2y + xy^2 + y^3 = dz^p. \tag{2.12}$$

Dans toute cette partie, on fait l'hypothèse suivante :

l'entier d libre de puissance troisième.

Sous cette hypothèse, si (a,b,c) appartient à $S_p(d)$, alors les entiers a, b et c sont premiers entre eux deux-à-deux.

En utilisant la courbe E d'équation (2.8) associée un élément de $S_p(d)$, et la méthode modulaire (dont le principe est résumé au début du paragraphe 2.2.3), on démontre plusieurs résulats sur l'équation (2.12).

Le premier concerne le cas $d = 1$.

Théorème 2.12 *Soit (a,b,c) un élément de $S_p(1)$. Alors, l'entier c est impair.*

Pour certaines valeurs de l'entier d, on a un résultat complet.

Théorème 2.13 *Les ensembles $S_p(2)$, $S_p(6)$, $S_p(10)$ et $S_p(22)$ sont vides.*

Soit ℓ est un nombre premier ≥ 13. On souhaite montrer, comme au théorème précédent pour $\ell = 3$, 5 et 11, la vacuité de l'ensemble $S_p(2\ell)$ (au-moins lorsque p est grand). Cela sera le cas si ℓ vérifie certaines conditions. Plus précisément, on désigne par g la fonction définie sur $\mathbf{N}^*$ par

$$g(n) = \begin{cases} \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n < 2^9, \\ 18 + 2\frac{\log n}{\log 2} & \text{si } 2^9 \leq n < 2^{362} \\ \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n \geq 2^{362}. \end{cases}$$

On dira que ℓ satisfait à la propriété (P) si pour tout entier k vérifiant l'inégalité

$$2 \leq k < g(\ell),$$

aucun des entiers $\ell - 1$, $\ell - 2^k$, $\ell + 2^k$ et $2^k - \ell$ n'est un carré.

On a alors le résultat suivant.

Théorème 2.14 *On suppose que ℓ vérifie la propriété (P). Il existe une constante $\kappa(\ell)$ ne dépendant que de ℓ telle que si $p > \kappa(\ell)$, alors l'ensemble $S_p(2\ell)$ est vide.*

Remarque 2.15 *On peut par exemple prendre $\kappa(\ell) = \left(4\sqrt{\ell+1} + 1\right)^{4(\ell-1)}$. L'amélioration de cette borne est, dans la pratique, limitée par la connaissance des newform (au sens de [AL70]) de poids 2 et de niveau 64ℓ. Par exemple, pour $\ell = 11$, on a $\kappa(11) \approx 7 \cdot 10^{46}$, alors que $S_p(22)$ est vide pour $p \geq 7$ d'après le théorème 2.13. Les nombres premiers $13 \leq \ell \leq 200$ satisfaisant à la condition (P) sont*

$$\ell = 19, 43, 59, 61, 67, 83, 107, 109, 131, 139, 149, 157, 163, 167, 179, 181 \text{ et } 191.$$

La suite de la partie 2.2 est consacrée à la démonstration des théorèmes 2.12, 2.13 et 2.14.

2.2.1 La courbe elliptique E

Soit (a, b, c) un élément de $S_p(d)$. À un tel triplet on associe la courbe elliptique $E/\mathbf{Q}$ définie par l'équation (2.8) avec $t_0 = t_1 = t_2 = t_3 = 1$:

$$y^2 = x^3 + (a-b)x^2 + (a+b)^2 x + a^3 + a^2 b - ab^2 - b^3. \tag{2.13}$$

La courbe E possède un unique point d'ordre 2 rationnel sur $\mathbf{Q}$, à savoir $(b-a, 0)$.

On a $\mathfrak{D}(f) = -16$ et les invariants standard (c_4, c_6, Δ) associés à E sont les suivants (cf. (2.9) et [Tat75]) :

$$\left\{ \begin{array}{lcl} c_4 & = & -32(a^2 + 4ab + b^2), \\ c_6 & = & -128(5a^3 + 3a^2 b - 3ab^2 - 5b^3), \\ \Delta & = & -2^8 F(a,b)^2 = -2^8 c^{2p} d^2. \end{array} \right. \tag{2.14}$$

Rappelons que N_E désigne le conducteur de E et Δ_E son discrimant minimal. Posons

$$r = \prod_{\ell | cd, \ell \neq 2} \ell.$$

Lemme 2.16 *La courbe E est semi-stable en dehors de 2. Elle a réduction additive en 2. L'équation (2.13) est globalement minimale.*

1. *Supposons d impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a*

$$N_E = \left\{ \begin{array}{ll} 2^6 r & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 r & \text{si } ab \text{ est pair.} \end{array} \right.$$

   L'invariant modulaire j de E est entier en 2 si et seulement si ab est pair.

2. *Supposons $v_2(d) = 1$. Alors on a*

$$ab \equiv -1 \pmod 4 \quad \text{et} \quad N_E = 2^6 r.$$

   L'invariant modulaire j de E n'est pas entier en 2.

3. *Supposons $v_2(d) = 2$. Alors ab est impair et on a*

$$N_E = \left\{ \begin{array}{ll} 2^5 r & \text{si } ab \equiv 1 \pmod 4, \\ 2^6 r & \text{si } ab \equiv -1 \pmod 4. \end{array} \right.$$

   L'invariant modulaire j de E est entier en 2 si et seulement si $ab \equiv 1 \pmod 4$.

De plus, si ℓ est un nombre premier impair, alors p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

DÉMONSTRATION : Soit ℓ un nombre premier impair. Supposons tout d'abord que l'entier ℓ divise Δ. D'après l'expression (2.14) ci-dessus, l'entier ℓ divise alors

$$F(a,b) = (a+b)(a^2 + b^2) = dc^p. \tag{2.15}$$

Remarquons que ℓ ne divise pas ab. Dans le cas contraire, l'entier a, par exemple, serait divisible par ℓ. Cela entrainerait que ℓ divise b (car ℓ divise $F(a,b)$) ce qui est contraire au fait que les entiers a et b sont premiers entre eux.

On en déduit que ℓ ne divise pas c_4. En effet, on a

$$c_4 \equiv \begin{cases} -2^6 ab \pmod{\ell} & \text{si } \ell \text{ divise } a+b, \\ -2^7 ab \pmod{\ell} & \text{si } \ell \text{ divise } a^2+b^2. \end{cases}$$

L'équation (2.13) est donc minimale en ℓ et la courbe E a mauvaise réduction de type multiplicatif en ℓ. On a $v_\ell(\Delta) = v_\ell(\Delta_E)$.

D'autre part, si ℓ ne divise pas Δ, la courbe E a bonne réduction en ℓ et l'équation (2.13) est minimale en ℓ.

Par ailleurs, on a dans les deux cas,

$$v_\ell(\Delta_E) = v_\ell(\Delta) \equiv 2v_\ell(d) \pmod{p}.$$

En particulier, p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

Étudions à présent la minimalité de (2.13) et le type de réduction de E en 2.

1. Supposons ab impair. Alors,

$$F(a,b) \equiv 2(a+b) \pmod{8} \quad \text{et} \quad v_2(c_4) = 6.$$

   (a) Si $ab \equiv 1 \pmod 4$, alors $v_2(F(a,b)) = 2$ donc nécessairement $v_2(d) = 2$ et c est impair. On vérifie que l'on a

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (6, \geq 9, 12). \tag{2.16}$$

   D'après le tableau II de [Pap93], l'équation (2.13) est minimale en 2 et on est dans le cas I_ν^* avec $\nu = 2$ ou $\nu = 3$. Avec l'algorithme de Tate ([Tat75, p.50]) on trouve $\nu = 3$ et on a $v_2(N_E) = 5$. De plus, l'invariant j est entier en 2 dans ce cas.

   (b) Si $ab \equiv -1 \pmod 4$, alors $v_2(F(a,b)) \geq 3$, donc c est pair. De plus,

$$v_2(\Delta) = 8 + 2v_2(d) + 2pv_2(c) \geq 22.$$

   Par ailleurs, on a

$$-\frac{c_6}{128} \equiv 5a + 3b - 3a - 5b \equiv 4a \pmod 8.$$

   On en déduit

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (6, 9, \geq 22).$$

   D'après [Pap93], l'équation (2.13) est minimale en 2 et on a $v_2(N_E) = 6$. L'invariant j n'est pas entier en 2.

2. Supposons ab pair. La solution (a,b,c) étant propre, a est pair et b impair (ou a est impair et b pair). On en déduit que c et d sont nécessairement impairs. D'où

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (5, 7, 8). \tag{2.17}$$

   D'après [Pap93], l'équation (2.13) est minimale en 2 et on a $v_2(N_E) = 7$. L'invariant j de E est entier en 2.

D'où le résultat.

2.2.2 La représentation ρ_p^E

Lemme 2.17 *La représentation ρ_p^E est (absolument) irréductible.*

DÉMONSTRATION : La courbe E a un point d'ordre 2 rationnel sur $\mathbf{Q}$, donc d'après le lemme 2.7, la représentation ρ_p^E est irréductible pour $p \geq 11$. Posons $t = a/b$. Alors, l'égalité $j = -15^3$ ou 255^3 (où j est l'invariant modulaire de E) conduit à

$$2^7 \frac{(t^2+4t+1)^3}{t^3+t^2+t+1} = -15^3 \quad \text{ou} \quad 255^3.$$

Or ces équations n'ont pas de solution rationnelle comme on le vérifie facilement. Cela démontre l'irréductibilité de ρ_7^E et le lemme.

Lemme 2.18 *On a $k = 2$ si p ne divise pas d et $k = p+1$ sinon.*

DÉMONSTRATION : Supposons que p ne divise pas d. Alors d'après les lemmes 2.8 et 2.16, on a $k = 2$.

Supposons que p divise d. D'après le lemme 2.16, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_E)$. Cela conduit à $k = p+1$, d'où le résultat.

Posons

$$r' = \prod_{\ell \mid d, \ell \neq 2, p} \ell.$$

Lemme 2.19 *1. On suppose que d est impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a*

$$N(\rho_p^E) = \begin{cases} 2^6 r' & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 r' & \text{si } ab \text{ est pair.} \end{cases}$$

2. On suppose que $v_2(d) = 1$. Alors on a

$$ab \equiv -1 \pmod 4 \quad \text{et} \quad N(\rho_p^E) = 2^6 r'.$$

3. On suppose que $v_2(d) = 2$. Alors ab est impair et on a

$$N(\rho_p^E) = \begin{cases} 2^5 r' & \text{si } ab \equiv 1 \pmod 4, \\ 2^6 r' & \text{si } ab \equiv -1 \pmod 4. \end{cases}$$

DÉMONSTRATION : Soit $\ell \neq p$ un nombre premier impair de mauvaise réduction. D'après le lemme 2.16, ℓ divise cd, l'équation (2.13) est minimale en ℓ et E a mauvaise réduction de type multiplicatif en ℓ.

Supposons que ℓ ne divise pas d. Alors, $v_\ell(\Delta_E)$ est multiple de p (*loc. cit.*). On en déduit que $v_\ell(N(\rho_p^E)) = 0$ ([Kra97a, p.28]).

Supposons que ℓ divise d. Alors, $v_\ell(\Delta_E)$ n'est pas multiple de p (lemme 2.16) et on a $v_\ell(N(\rho_p^E)) = 1$ ([Kra97a, p.28]).

D'après le lemme 2.16, la courbe E a donc réduction additive en 2 et on a $v_2(N(\rho_p^E)) = v_2(N_E)$ (*loc. cit.*). D'où le lemme.

2.2.3 Démonstrations des théorèmes 2.12, 2.13 et 2.14

On suppose dans tout ce paragraphe qu'il existe $(a,b,c) \in S_p(d)$ où p est un nombre premier ≥ 7 et d l'un des entiers considérés dans les énoncés des théorèmes 2.12, 2.13 et 2.14.

Notations et rappels. Soit $n \in \mathbf{N}^*$. On désigne par $\mathcal{S}_2^+(n)$ l'espace des newform (au sens de [AL70]) de poids 2 pour le sous-groupe $\Gamma_0(n)$ de $\mathrm{SL}_2(\mathbf{Z})$. On dit que $f \in \mathcal{S}_2^+(n)$ est normalisée si son développement de Fourier à l'infini s'écrit

$$f = q + \sum_{m \geq 2} a_m(f) q^m, \quad \text{avec } q = e^{2i\pi\tau}.$$

Il y a exactement $\dim_{\mathbf{C}}(\mathcal{S}_2^+(n))$ formes normalisées dans $\mathcal{S}_2^+(n)$. Pour une telle forme, notons K_f le corps de rationalité des coefficients $a_m(f)$, $m \geq 2$ et $\mathrm{N}_{K_f/\mathbf{Q}}$ la norme de l'extension $K_f/\mathbf{Q}$.

Si $A/\mathbf{Q}$ est une courbe elliptique, on note

$$L_A(s) = \sum_{m \geq 0} a_m(A) m^{-s}$$

sa fonction L de Hasse-Weil.

Rappelons le résultat bien connu suivant (cf. par exemple [Ser96]).

Proposition 2.20 *Il existe $f \in \mathcal{S}_k^+(N(\rho_p^E))$ normalisée telle que pour tout nombre premier ℓ, les conditions suivantes soient réalisées.*

1. *Si ℓ divise N_E et ne divise pas $pN(\rho_p^E)$, alors*

$$p \text{ divise } \mathrm{N}_{K_f/\mathbf{Q}}(a_\ell(f) \pm (\ell+1)).$$

2. *Si ℓ ne divise pas pN_E, alors il existe un entier $r \leq \sqrt{l}$ tel que*

$$p \text{ divise } \mathrm{N}_{K_f/\mathbf{Q}}(a_\ell(f) \pm 2r).$$

Pour l'assertion 2, on utilise le fait que, comme E a un point d'ordre 2 rationnel sur $\mathbf{Q}$, le coefficient $a_\ell(E)$ est pair. On a de plus $|a_\ell(E)| \leq 2\sqrt{\ell}$ d'après les bornes de Weil.

Si f, vérifiant les conditions de la proposition 2.20, a ses coefficients $a_m(f)$ dans $\mathbf{Z}$, alors elle correspond à une courbe elliptique E_f de conducteur $N(\rho_p^E)$ définie sur $\mathbf{Q}$ et les représentations ρ_p^E et $\rho_p^{E_f}$ sont isomorphes.

Soit $\mathbf{Q}(E[p])/\mathbf{Q}$ l'extension de $\mathbf{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbf{Q}$. Soit e son indice de ramification en 2.

Lemme 2.21 *Supposons $ab \equiv -1 \pmod 4$. On a $e = 2p$.*

DÉMONSTRATION : Supposons $ab \equiv -1 \pmod 4$. D'après lemme 2.16, l'invariant modulaire j de E n'est pas entier en 2. De plus, on a

$$v_2(j) = 18 - (8 + 2v_2(d) + 2pv_2(c)) \equiv 10 - 2v_2(d) \not\equiv 0 \pmod p$$

car $v_2(d) = 0$ ou 1 par hypothèse. On en déduit $e = 2p$ ([CK02, cor. 1]).

Démonstration du théorème 2.12

Supposons $d = 1$. D'après le lemme 2.19, on a

$$N(\rho_p^E) = \begin{cases} 2^6 & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 & \text{si } ab \text{ est pair.} \end{cases}$$

Supposons $ab \equiv -1 \pmod 4$. L'espace $\mathcal{S}_2^+(64)$ n'est constitué que d'une seule classe de $\mathbf{Q}$-isogénie de courbe elliptique de conducteur 64. Par ailleurs, la courbe E a potentiellement réduction multiplicative en 2 et son défaut de semi-stabilité en 2 est d'ordre $2p$ (lemme 2.21). Or, les courbes de conducteur 64 ont réduction additive en 2 et leur invariant modulaire est entier. Si A est une telle courbe, l'indice de ramification en 2 de l'extension $\mathbf{Q}(A[p])/\mathbf{Q}$ est 8 (cf. [Cre97] et [Kra90]). Les représentations ρ_p^E et ρ_p^A ne sont donc pas isomorphes. On en déduit que ab est pair. D'où le théorème 2.12.

Démonstration du théorème 2.13

Supposons que $d \in \{2, 6, 10, 22\}$. D'après le lemme 2.19, on a $ab \equiv -1 \pmod 4$ et

$$N(\rho_p^E) = \begin{cases} 2^6 & \text{si } d = 2, \\ 2^6 \cdot 3 & \text{si } d = 6, \\ 2^6 \cdot 5 & \text{si } d = 10, \\ 2^6 \cdot 11 & \text{si } d = 22 \text{ et } p \neq 11, \\ 2^6 & \text{si } d = 22 \text{ et } p = 11. \end{cases}$$

De plus, d'après le lemme 2.21, on a $e = 2p$.

Supposons $d = 2$. On a alors $N(\rho_p^E) = 64$. On montre, avec le même argument qu'au paragraphe 2.2.3, que l'ensemble $S_p(2)$ est vide.

Supposons $d = 6$. L'espace $\mathcal{S}_2^+(192)$ est de dimension 4 et engendré par quatre classes de $\mathbf{Q}$-isogénie de courbes elliptiques définies sur $\mathbf{Q}$ (cf. [Ste06]). Toutes ont réduction additive en 2 et un invariant modulaire entier en 2. Leur défaut de semi-stabilité en 2 est d'ordre 8 ou 24 (cf. [Cre97] et [Kra90]). En particulier, il est différent de $2p$. On en déduit que l'ensemble $S_p(6)$ est vide.

Supposons $d = 10$. L'espace $\mathcal{S}_2^+(320)$ est engendré par six classes de $\mathbf{Q}$-isogénie de courbes elliptiques de conducteur 320 et deux formes modulaires f_1 et f_2 dont les coefficients de Fourier sont conjugués sur $\mathbf{Q}(\sqrt{2})$ (cf. [Ste06]). La forme $f = f_1$ ou f_2 est à coefficients dans l'anneau d'entiers du corps K_f engendré sur $\mathbf{Q}$ par une racine α du polynôme $X^2 - 8$ (*loc. cit.*). Avec les notations de la proposition 2.20, on a pour $\ell = 3$, le tableau suivant.

$a_3(f)$	$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) \pm 4)$	$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f))$	$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) \pm 2)$
α	8	-8	-4

La forme f ne vérifie donc pas les conditions de la proposition 2.20. On en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbf{Q}$ de conducteur 320. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2 (leur défaut de semi-stabilité en 2 divise 24 d'après [Ser72, p.386], en particulier il est différent de $2p$). L'ensemble $S_p(10)$ est donc vide.

Supposons $d = 22$ et $p \neq 11$. L'espace $\mathcal{S}_2^+(704)$ est constitué de douze classes de $\mathbf{Q}$-isogénie de courbes elliptiques de conducteur 704 et de huit formes modulaires. Chacune de ces huit formes est conjuguée par l'action de $\mathrm{G}_{\mathbf{Q}}$ à l'une des quatre formes notées 704M1, 704N1, 704O1 et 704P1 dans [Ste06]. Avec les notations de la proposition 2.20, on a le tableau suivant pour $\ell = 3$.

Newform f	704M1	704N1	704O1	704P1
Polynôme P_f tel que $K_f = \mathbf{Q}(\alpha)$ et $P_f(\alpha) = 0$	$X^2 + X - 4$	$X^2 - X - 4$	$X^2 + X - 4$	$X^2 - X - 4$
$a_3(f)$	α	α	α	α
$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) + 4)$	8	16	8	16
$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) - 4)$	16	8	16	8
$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f))$	-4	-4	-4	-4
$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) + 2)$	-2	2	-2	2
$\mathrm{N}_{K_f/\mathbf{Q}}(a_3(f) - 2)$	2	-2	2	-2

Aucune de ces formes ne vérifiant les conditions de la proposition 2.20, on en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbf{Q}$ de conducteur 704. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2. L'ensemble $S_p(22)$ est donc vide dans ce cas.

Supposons $d = 22$ et $p = 11$. La représentation ρ_{11}^E est irréductible, de poids 12 (lemme 2.18) et de conducteur 64. Je remercie le referee de m'avoir signalé que ρ_{11}^E « provient » alors d'une newform de poids 2 et de niveau $12 \cdot 64 = 704$ (voir [Rib94, (2.2)] et [Dia95, lem. 2.1]). Autrement dit, de façon analogue à la proposition 2.20, il existe $f \in \mathcal{S}_2^+(12 \cdot 64)$ normalisée telle pour tout nombre premier $\ell \neq 2, 11$, les conditions suivantes soient réalisées :

1. si ℓ divise N_E, alors 11 divise $\mathrm{N}_{K_f/\mathbf{Q}}(a_\ell(f) \pm (\ell + 1))$.
2. Il existe un entier $r \leq \sqrt{l}$ tel que 11 divise $\mathrm{N}_{K_f/\mathbf{Q}}(a_\ell(f) \pm 2r)$.

On contredit alors l'existence d'une telle forme par les mêmes arguments qu'à l'alinéa précédent. On en déduit que l'ensemble $S_{11}(22)$ est vide.

Cela démontre le théorème 2.13.

Démonstration du théorème 2.14

Supposons $d = 2\ell$, où ℓ est un nombre premier ≥ 13 satisfaisant à la propriété (P). La représentation ρ_p^E est alors irréductible pour $p \geq 7$ et de poids 2 dès que $p \neq \ell$ (lemmes 2.17 et 2.18). On a alors $ab \equiv -1 \pmod 4$ et $N(\rho_p^E) = 2^6\ell$.

D'après [Kra97b, th.3], il existe une constante $\kappa(\ell) > \ell$ ne dépendant que de ℓ vérifiant la condition suivante : si $p > \kappa(\ell)$, alors il existe une courbe elliptique E' définie sur $\mathbf{Q}$, de conducteur $N(\rho_p^E) = 2^6\ell$, telle que les représentations ρ_p^E et $\rho_p^{E'}$ soient isomorphes.

Quitte à augmenter $\kappa(\ell)$, on peut de plus supposer que E' a un point d'ordre 2 rationnel sur $\mathbf{Q}$ (cf. démonstration du th. 4 de [Kra97b] et [Ser68, IV-6]).

Lorsqu'il n'existe pas de courbe elliptique sur $\mathbf{Q}$ de conducteur 64ℓ ayant au-moins un point d'ordre 2 rationnel sur $\mathbf{Q}$, on a une contradiction. Or c'est précisément le cas lorsque ℓ vérifie la propriété (P) d'après un théorème de W. Ivorra (cf. [Ivo04]). D'après [Kra97b], on peut prendre $\kappa(\ell) = \left(4\sqrt{\ell + 1} + 1\right)^{4(\ell-1)}$. On en déduit le théorème 2.14.

Remarque 2.22 *Pour caractériser l'existence de courbe elliptique sur* $\mathbf{Q}$ *ayant un point d'ordre deux rationnel sur* $\mathbf{Q}$ *et un conducteur* 64ℓ*, Ivorra ([Ivo04]) utilise les bornes données par Beukers (corollaires* 1 *et* 2 *de [Beu81]) sur les solutions de l'équation de Ramanujan-Nagell. Ces bornes ont depuis été améliorées par Bauer et Bennett ([BB02]). Notre définition de la fonction* g *prend en compte ces améliorations (lorsque* $2^9 \leq n < 2^{362}$ *on a adapté la démonstration du corollaire* 2 *de [Beu81] aux nouvelles bornes).*

2.3 Remarques en degré ≥ 3

2.3.1 Courbe de Frey en degré 6

Soit F un polynôme homogène de degré 6 séparable à coefficients entiers. Sous certaines conditions portant sur F, on peut, comme à la partie 2.1, construire une courbe elliptique ayant de bonnes propriétés de réduction, associée à l'équation (2.1).

Par exemple, pour $F(x,y) = \Phi_9(x,y) = x^6 + x^3y^3 + y^6$, on obtient la courbe elliptique suivante :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 &= 3ab, \\ a_4 &= -3(a^4 - a^3b + 2a^2b^2 - ab^3 + b^4), \\ a_6 &= a^6 - 9a^5b + 9a^4b^2 - 19a^3b^3 + 9a^2b^4 - 9ab^5 + b^6. \end{cases}$$

Son discriminant est $\Delta = 2^4 \cdot 3^4 \cdot \Phi_9(a,b)^2$. Elle est semi-stable en dehors de 2 et 3. Une telle courbe devrait permettre d'obtenir des résultats analogues à ceux de la partie 2.2 pour la forme $F = \Phi_9$.

2.3.2 Détermination des solutions entières de certaines équations superelliptiques

Dans les parties 2.1 et 2.2, on a associé une courbe de Frey à une équation diophantienne donnée. On illustre ici sur un exemple la possibilité de montrer la vacuité de l'ensemble des solutions d'une équation en partant de la donnée d'une courbe elliptique bien choisie.

Soit t une indéterminée. On considère la courbe $E/\mathbf{Q}[t]$ d'équation :

$$E : y^2 + txy = x^3 + (1+t)x.$$

Ses coefficients $\Delta(t)$ et $c_4(t)$ sont les éléments suivants de $\mathbf{Q}[t]$:

$$\Delta(t) = t^6 + 2t^5 + t^4 - 64t^3 - 192t^2 - 192t - 64,$$

$$c_4(t) = t^4 - 48t - 48.$$

De plus, si R désigne leur résultant, on a :

$$R = 2^{16}.$$

Autrement dit, après spécialisation en t entier, la courbe E est semi-stable en dehors de 2. Si t est divisible par 4, la valuation en 2 de $\Delta(t)$ est 6. De même, si $v_2(t) = 1$, alors $v_2(\Delta(t)) = 4$. Enfin, si t est impair, $\Delta(t)$ est pair et $c_4(t)$ impair.

Par ailleurs, $(0,0)$ est un point d'ordre 2 de E rationnel sur $\mathbf{Q}$. La représentation ρ_p^E est donc irréductible pour $p \geq 11$ (lemme 2.7). De plus, l'invariant modulaire j de E est différent de -15^3 et 255^3. On en déduit que ρ_7^E est également irréductible (*loc. cit.*).

On suppose à présent qu'il existe un entier c tel que t vérifie l'équation superelliptique :

$$\Delta(t) = c^p,$$

où p est un nombre premier ≥ 7. D'après les remarques ci-dessus, t est impair. Dans ce cas, la courbe E est semi-stable et la représentation ρ_p^E est de poids 2 et de conducteur 1. C'est absurde. Cela contredit l'existence de c.

2.4 Annexe A – La conjecture *abc* implique la conjecture (A)

Dans [Lan99a], M. Langevin montre que la conjecture *abc* est équivalente à la conjecture suivante.

Conjecture 2.23 *Soient $F \in \mathbf{Z}[X,Y]$ une forme homogène séparable de degré ≥ 3 et ε un réel > 0. Il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que pour tout couple (a,b) d'entiers non nuls premiers entre eux, on a :*

$$\mathrm{rad}(F(a,b)) \geq C_{\varepsilon,F} \max(|a|,|b|)^{\deg(F)-2-\varepsilon},$$

où $\mathrm{rad}(n)$, $n \in \mathbf{N}^*$, *désigne le produit de tous les nombres premiers divisant n.*

Remarque. Par convention $\mathrm{rad}(0) = \infty$.

L'objectif ce cette *Annexe* est d'une part de démontrer le résultat de Langevin en suivant une méthode géométrique esquissée dans l'article de [GT02] (voir également [Hin08, pp.244-246]) et d'autre part d'en déduire la conjecture (A).

2.4.1 Le résultat de Langevin

On commence par rappeler l'énoncé de la conjecture *abc* sous sa forme classique.

Conjecture 2.24 (*abc*) *Soit ε un réel > 0. Il existe une constante $C(\varepsilon) > 0$ telle que pour tout triplet (a,b,c) d'entiers non nuls premiers entre eux vérifiant $a+b=c$, on ait*

$$\mathrm{rad}(abc) \geq C(\varepsilon) \max(|a|,|b|)^{1-\varepsilon}.$$

L'objectif de ce § est de démontrer la proposition suivante.

Proposition 2.25 *La conjecture* abc *est équivalente à la conjecture 2.23.*

La conjecture 2.23 implique la conjecture *abc* : il suffit de prendre

$$F(X,Y) = XY(X+Y).$$

Intéressons-nous donc à la réciproque. La démonstration requiert plusieurs étapes.

1. Le théorème de Mason

Notation. Étant donné un polynôme $f \in \mathbf{Z}[X]$, la notation $\{f = 0\}$ désigne l'ensemble des racines complexes de f. En particulier, $|\{f = 0\}|$ est le nombre de racines de f comptées sans multiplicité.

Théorème 2.26 (Mason) *Soient a, b et c trois polynômes de $\mathbf{Z}[t]$ non constants et premiers entre eux vérifiant :*

$$a(t) + b(t) = c(t).$$

Alors, on a :

$$\max(\deg(a), \deg(b), \deg(c)) \leq |\{abc = 0\}| - 1. \tag{2.18}$$

Démonstration. On considère a, b et c comme dans l'énoncé du théorème. L'application

$$\phi \ : t \mapsto \frac{a(t)}{c(t)}$$

est une application rationnelle $\mathbf{P}^1 \to \mathbf{P}^1$ non constante définie sur $\mathbf{Q}$. De plus, remarquons que

- si $\phi(\infty) \neq 0$, alors $\phi^{-1}(0) = \{a = 0\}$
- si $\phi(\infty) \neq \infty$, alors $\phi^{-1}(\infty) = \{c = 0\}$,
- si $\phi(\infty) \neq 1$, alors $\phi^{-1}(1) = \{b = 0\}$.

Par ailleurs, ∞ appartient à l'un, au plus, des ensembles $\phi^{-1}(\infty)$, $\phi^{-1}(1)$ et $\phi^{-1}(0)$. Appliquons à présent la formule de Riemann - Hurwitz à ϕ qui est de degré $d = \max(\deg(a), \deg(c))$. On a :

$$-2 = -2d + \sum_{y \in \mathbf{P}^1} \left(d - |\phi^{-1}(y)|\right).$$

Chacun des termes de la somme (finie) du membre de droite de l'égalité ci-dessus étant ≥ 0, on a la minoration suivante :

$$-2 \geq -2d + \sum_{y \in \{0,1,\infty\}} \left(d - |\phi^{-1}(y)|\right). \tag{2.19}$$

(Avec égalité si ϕ est non ramifiée hors de $\{0, 1, \infty\}$.) On en déduit

$$-2 \geq -2d + 3d - \left(|\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)|\right).$$

Soit encore

$$d \leq |\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)| - 2.$$

Or, les polynômes a, b et c étant premiers entre eux on a d'après ce qui précède :

$$|\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)| \leq |\{abc = 0\}| + 1. \tag{2.20}$$

(Avec égalité si $\phi(\{\infty\}) \subset \{0, 1, \infty\}$.) On en déduit l'inégalité

$$d \leq |\{abc = 0\}| - 1.$$

Comme par ailleurs, $b = c - a$, on a

$$\deg(b) \leq d$$

puis $d = \max(\deg(a), \deg(b), \deg(c))$. D'où le résultat.

2. Le théorème de Belyi

Adoptons la définition usuelle suivante.

Définition 2.27 *Soit S un ensemble fini de $\mathbf{P}^1(\overline{\mathbf{Q}})$. On appelle fonction de Belyi associée à S toute application rationnelle non constante $\phi : \mathbf{P}^1 \to \mathbf{P}^1$ définie sur $\mathbf{Q}$ vérifiant les propriétés suivantes :*

1. *la fonction ϕ est non ramifiée hors de 0, 1 et ∞ ;*
2. *on a $\phi(S) \subset \{0, 1, \infty\}$.*

Concernant l'existence de telles fonctions on a le résultat suivant (*cf.* [Ser97]).

Théorème 2.28 (Belyi) *Soit $S \subset \mathbf{P}^1(\overline{\mathbf{Q}})$ un ensemble fini. Alors, il existe une fonction de Belyi associée à S.*

Vu la démonstration du théorème de Mason donnée ci-dessus, on a le lemme suivant.

Lemme 2.29 *Soit ϕ une fonction de Belyi associée à $\{\infty\}$ et $a(t)$, $c(t)$ deux polynômes de $\mathbf{Z}[t]$ non constants et premiers entre eux tels que $\phi(t) = a(t)/c(t)$. Alors, on a l'égalité*

$$\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1,$$

où l'on a posé $b(t) = c(t) - a(t)$.

Démonstration. Dans la démonstration du théorème 2.26, on a deux inégalités dont résulte celle du théorème : (2.19) et (2.20). On a égalité dans (2.19) si ϕ est non ramifiée hors de $\{0, 1, \infty\}$. On a égalité dans (2.20) si $\phi(\{\infty\}) \subset \{0, 1, \infty\}$. Or c'est bien le cas par définition d'une fonction de Belyi. D'où le lemme.

3. Sur certains cas d'égalité dans le théorème de Mason

Proposition 2.30 *Soit $f \in \mathbf{Z}[t]$ un polynôme séparable. Alors, il existe $a(t)$, $b(t)$ et $c(t)$ trois polynômes non constants de $\mathbf{Z}[t]$ premiers entre eux tels que :*

1. *$a(t) + b(t) = c(t)$;*
2. *$\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1$;*
3. *deux des trois polynômes a, b et c sont de même degré et le troisième est de degré strictement plus petit ;*
4. *le polynôme f divise abc.*

Démonstration. Soit $S = \{f = 0\} \cup \{\infty\}$. C'est un sous-ensemble fini de $\mathbf{P}^1(\overline{\mathbf{Q}})$. D'après le théorème 2.28, il existe une fonction de Belyi ϕ associée à S. Posons, $\phi = a/c$, où a et c sont deux polynômes de $\mathbf{Z}[t]$ premiers entre eux et non constants, puis $b = c - a$. Comme $\{\infty\} \subset S$, l'application ϕ est en particulier une fonction de Belyi asscoiée à $\{\infty\}$. D'après le lemme 2.29, les polynômes a, b et c satisfont aux conditions 1 et 2.

Notons $d = \max(\deg(a), \deg(b), \deg(c))$. D'après la condition 1, les trois polynômes a, b et c ne sont pas tous de degrés différents. Il y en a donc au moins deux de même de degré, et c'est d. Par ailleurs, on a supposé que $\infty \in S$, et donc $\phi(\infty) = 0$, 1 ou ∞. Autrement dit, il y a au plus deux des trois polynômes

a, b et c qui sont de même degré. Finalement, parmi les trois polynômes a, b et c, deux exactement sont de même degré d. C'est la condition 3.

Par ailleurs, soit $t \in \mathbf{P}^1(\overline{\mathbf{Q}})$ tel que $f(t) = 0$. Alors, par définition, on a $t \in S$. Comme ϕ est une fonction de Belyi pour S, on a $\phi(t) = 0$, 1 ou ∞. Autrement dit, t vérifie :

$$(abc)(t) = 0.$$

Le polynôme f étant séparable on en déduit qu'il divise le produit abc. Cela démontre la proposition.

4. Fin de la démonstration

On considère F comme dans la conjecture 2.23 et on pose $f(t) = F(t, 1)$. Le polynôme f est séparable de degré

$$\deg(f) \geq \deg(F) - 1. \tag{2.21}$$

Soient m et n deux entiers non nuls et premiers entre eux tels que $F(m, n) \neq 0$.

Quitte à changer $F(X, Y)$ en $F(Y, X)$, on peut supposer que l'on a $m \leq n$. De même, quitte à changer $F(X, Y)$ en $F(-X, Y)$, on peut supposer que l'on a $m > 0$. On suppose donc à partir de maintenant que l'on a

$$0 < m \leq n.$$

Le polynôme f étant séparable, il existe d'après la proposition 2.30, trois polynômes a, b et c non constants de $\mathbf{Z}[t]$ premiers entre eux tels que :

1. $a(t) + b(t) = c(t)$;
2. $\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1$;
3. deux des trois polynômes a, b et c sont de même degré et le troisième est de degré strictement plus petit ;
4. le polynôme f divise abc.

Posons $d = \max(\deg(a), \deg(b), \deg(c))$ et homogénéisons les polynômes a, b et c en degré d :

$$\begin{aligned} A(X, Y) &= Y^d a(X/Y), \\ B(X, Y) &= Y^d b(X/Y), \\ C(X, Y) &= Y^d c(X/Y). \end{aligned}$$

D'après la condition 1, on a

$$A(m, n) + B(m, n) = C(m, n).$$

Les entiers $A(m, n)$, $B(m, n)$ et $C(m, n)$ ne sont pas nécessairement premiers entre eux. Notons D leur pgcd.

Lemme 2.31 *L'entier D est majoré indépendamment de m et n.*

Démonstration. Quitte à échanger les polynômes a, b et c, on peut supposer (dans cette démonstration) que l'on a

$$\deg a = \deg b = d.$$

Posons alors

$$a(t) = a_0 t^d + \cdots + a_d \quad \text{et} \quad b(t) = b_0 t^d + \cdots + b_d.$$

Par définition, le résultant de a et b ([Bou81, A IV.71]), noté $\mathrm{Res}(a,b)$, est le déterminant de la matrice de Sylvester M de a et b (de taille $(2d)\times(2d)$) rappelée ci-dessous :

$$M = \begin{pmatrix} a_0 & \dots & \dots & \dots & a_d & & & 0 \\ 0 & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ & & \ddots & & \vdots & & \ddots & \\ & & & a_0 & a_1 & \dots & \dots & a_d \\ b_0 & \dots & \dots & \dots & b_d & & & \\ 0 & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ & & \ddots & & \vdots & & \ddots & \\ 0 & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

On note $\{C_i\}_{1\le i\le 2d}$ les colonnes de la matrice M. D'après les propriétés du déterminant, on a

$$X^{2d-1}\mathrm{Res}(a,b) = \det \begin{pmatrix} X^{2d-1}a_0 & \dots & \dots & \dots & a_d & & & 0 \\ 0 & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ & & \ddots & & \vdots & & \ddots & \\ & & & a_0 & a_1 & \dots & \dots & a_d \\ X^{2d-1}b_0 & \dots & \dots & \dots & b_d & & & \\ 0 & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ & & \ddots & & \vdots & & \ddots & \\ 0 & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

Puis, en ajoutant à la première colonne de la matrice ci-dessus $X^{2d-i}Y^{i-1}C_i$ pour tout $2 \le i \le 2d$, on ne modifie pas la valeur du déterminant, et on obtient ainsi

$$X^{2d-1}\mathrm{Res}(a,b) = \det \begin{pmatrix} X^{d-1}A(X,Y) & \dots & \dots & \dots & a_d & & & 0 \\ X^{d-2}YA(X,Y) & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ Y^{d-1}A(X,Y) & & & a_0 & a_1 & \dots & \dots & a_d \\ X^{d-1}B(X,Y) & \dots & \dots & \dots & b_d & & & \\ X^{d-2}YB(X,Y) & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ Y^{d-1}B(X,Y) & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

D'où, en développant le déterminant ci-dessus par rapport à la première colonne :

$$X^{2d-1}\mathrm{Res}(a,b) \in (A,B)\mathbf{Z}[X,Y].$$

En raisonnant comme ci-dessus (en remplaçant la colonne C_{2d} de la matrice M par $Y^{2d-1}C_{2d}$ et en ajoutant à celle-ci la somme des colonnes $X^{2d-i}Y^{i-1}C_i$ pour $1 \le i \le 2d-1$), on montre de même que l'on a

$$Y^{2d-1}\mathrm{Res}(a,b) \in (A,B)\mathbf{Z}[X,Y].$$

Or, le pgcd D de $A(m,n)$, $B(m,n)$ et $C(m,n)$ est le même que celui de $A(m,n)$ et $B(m,n)$. Donc, en spécialisant les relations ci-dessus, on a en particulier,

$$D \mid n^{2d-1}\mathrm{Res}(a,b) \quad \text{et} \quad D \mid m^{2d-1}\mathrm{Res}(a,b).$$

Les entiers m et n étant premiers entre eux, on en déduit que D divise le résultant de a et b. L'entier D est donc majoré indépendamment de m et n. D'où le lemme 2.31.

Quitte à interchanger a, b et c, on peut supposer que l'on a $A(m,n) \geq 0$, $B(m,n) \geq 0$ et $C(m,n) \geq 0$.

D'après le lemme précédent, on peut appliquer la conjecture *abc* aux entiers positifs, $A(m,n)$, $B(m,n)$ et $C(m,n)$. Pour $\varepsilon > 0$, on obtient :

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \gg_{\varepsilon,F} \max(A(m,n),B(m,n))^{1-\varepsilon}. \tag{2.22}$$

La fin de la démonstration de la proposition 2.25 consiste à minorer convenablement le membre de droite de l'inégalité ci-dessus et majorer celui de gauche.

Majoration. Étant donné un polynôme H de l'anneau (factoriel) $\mathbf{Z}[X,Y]$, on désigne par $\mathrm{rad}(H)$ le polynôme (bien défini au signe près)

$$\mathrm{rad}(H) = \prod_{P \mid H} P,$$

où le produit porte sur les éléments irréductibles P de $\mathbf{Z}[X,Y]$.

On aura besoin du lemme suivant.

Lemme 2.32 *Le polynôme $F(X,Y)$ divise* $\mathrm{rad}(A(X,Y)B(X,Y)C(X,Y))$.

Démonstration. Par construction, le polynôme f divise le produit *abc*. Posons

$$(abc)(t) = f(t)\cdot g(t), \quad \text{où } \deg(g) = \deg(abc) - \deg(f).$$

On a

$$\begin{aligned} A(X,Y)B(X,Y)C(X,Y) &= Y^{3d}a\Big(\frac{X}{Y}\Big)b\Big(\frac{X}{Y}\Big)c\Big(\frac{X}{Y}\Big) \\ &= Y^{3d}f\Big(\frac{X}{Y}\Big)g\Big(\frac{X}{Y}\Big) \\ &= Y^{3d-\deg(F)}F(X,Y)g\Big(\frac{X}{Y}\Big). \end{aligned}$$

Or, par construction, deux seulement des polynômes a, b et c sont de degré d et le troisième est de degré $< d$. Donc on a

$$3d - \deg(F) \geq \deg(abc) - \deg(F) + 1,$$

puis d'après la formule (2.21)

$$3d - \deg(F) \geq \deg(abc) - \deg(f) = \deg(g).$$

Autrement dit, le polynôme

$$Y^{3d-\deg(F)}g\Big(\frac{X}{Y}\Big) \in \mathbf{Z}[X,Y]$$

et F divise le produit ABC. Or, F est séparable par hypothèse, donc F divise $\mathrm{rad}(ABC)$. D'où le lemme 2.32.

D'après le lemme 2.32, posons :

$$\mathrm{rad}(ABC) = F \cdot G,$$

où $G \in \mathbf{Z}[X, Y]$. On en déduit

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \mid \mathrm{rad}(ABC)(m,n) = F(m,n)G(m,n),$$

puis

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \leq \mathrm{rad}(F(m,n))|G(m,n)|. \tag{2.23}$$

Or, l'un des trois polynômes a, b et c est de degré $< d$ et les deux autres sont de degré excatement d, d'où

$$\deg(\mathrm{rad}(ABC)) = |\{abc = 0\}| + 1.$$

Or, par construction $|\{abc = 0\}| = d + 1$. D'où :

$$\deg(\mathrm{rad}(ABC)) = d + 2.$$

On en déduit que G est de degré $d + 2 - \deg(F)$. D'où

$$|G(m,n)| \ll_F \max(|m|, |n|)^{d+2-\deg(F)}$$

et la majoration suivante d'après l'inégalité (2.23)

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \ll_F \mathrm{rad}(F(m,n)) \max(|m|, |n|)^{d+2-\deg(F)}. \tag{2.24}$$

Minoration. On rappelle que l'on s'est placé dans la situation où

$$0 < m \leq n \quad \text{et} \quad A(m,n),\ B(m,n) \text{ et } C(m,n) \geq 0.$$

On a alors

$$\begin{aligned}
\max\left(A(m,n), B(m,n)\right) &= n^d \max\left(a\left(\frac{m}{n}\right), b\left(\frac{m}{n}\right)\right) \\
&= \max(|m|, |n|)^d \max\left(a\left(\frac{m}{n}\right), b\left(\frac{m}{n}\right)\right) \\
&\geq \max(|m|, |n|)^d \inf_{t \in \mathbf{C}} \big(\max\left(|a(t)|, |b(t)|\right)\big).
\end{aligned}$$

Or les polynômes a et b étant premiers entre eux, on a, d'après un lemme de K. Mahler (*cf.* [Lan99b]) rappelé ci-dessous,

$$\inf_{t \in \mathbf{C}} \big(\max\left(|a(t)|, |b(t)|\right)\big) > 0.$$

On en déduit la minoration suivante

$$\max\left(A(m,n), B(m,n), C(m,n)\right) \gg_F \max(|m|, |n|)^d. \tag{2.25}$$

Lemme 2.33 (Mahler) *Soient P et Q deux polynômes complexes sans zéro commun. Alors,*

$$\inf_{z\in\mathbf{C}}\big(\max\left(|P(z)|,|Q(z)|\right)\big)>0.$$

Démonstration. Posons

$$P(z)=a(z-x_1)\dots(z-x_p)\quad\text{et}\quad Q(z)=b(z-y_1)\dots(z-y_q).$$

Par hypothèse, $x_i\neq y_j$ pour tout i,j. Soit $z\in\mathbf{C}$. Supposons que l'on ait

$$\min_j|z-y_j|\geq\min_i|z-x_i|.$$

Soit alors i_0 tel que $|z-x_{i_0}|\leq\min_j|z-y_j|$. Alors, pour tout $1\leq j\leq q$, on a d'après l'inégalité triangulaire

$$|x_{i_0}-y_j|\leq|x_{i_0}-z|+|z-y_j|\leq 2|z-y_j|.$$

D'où $|Q(z)|\geq 2^{-q}|Q(x_{i_0})|$ puis

$$|Q(z)|\geq\min_{i,j}\big(2^{-p}|P(y_j)|,2^{-q}|Q(x_i)|\big).$$

Si $\min_j|z-y_j|<\min_i|z-x_i|$, on obtient de même

$$|P(z)|\geq\min_{i,j}\big(2^{-p}|P(y_j)|,2^{-q}|Q(x_i)|\big).$$

D'où

$$\max\left(|P(z)|,|Q(z)|\right)\geq\min_{i,j}\big(2^{-p}|P(y_j)|,2^{-q}|Q(x_i)|\big)>0.$$

Cela démontre le lemme car l'infimum d'un ensemble est le plus grand de ses minorants.

Conclusion. En combinant les inégalités (2.24) et (2.25), on obtient

$$\mathrm{rad}(F(m,n))\max(|m|,|n|)^{d+2-\deg(F)}\gg_{\varepsilon,F}\max(|m|,|n|)^{d(1-\varepsilon)}.$$

D'où le résultat en remplaçant ε par ε/d dans (2.22). Cela achève la démonstration de la proposition 2.25.

2.4.2 La conjecture *abc* implique la conjecture (A)

Déduisons à présent la conjecture (A) de la conjecture *abc* telle qu'elle est formulée au § précédent.

Proposition 2.34 *La conjecture abc implique la conjecture (A).*

Démonstration : Soient F une forme homogène séparable de degré ≥ 3 à coefficients entiers relatifs et d un entier ≥ 1. On considère (a,b,c) une solution propre et non triviale de (2.1). Posons

$$a'=\frac{a}{\mathrm{pgcd}(a,b)}\quad\text{et}\quad b'=\frac{b}{\mathrm{pgcd}(a,b)},$$

où $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b. Les entiers a, b et c étant premiers entre eux, on en déduit que $(\mathrm{pgcd}(a,b))^{\deg(F)}$ divise d. On a alors

$$F(a',b') = d'c^p, \quad \text{où } d' = \frac{d}{(\mathrm{pgcd}(a,b))^{\deg(F)}}. \tag{2.26}$$

Les entiers a' et b' étant premiers entre eux, on déduit de la conjecture ci-dessus que pour tout $\varepsilon > 0$, il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que

$$\mathrm{rad}(F(a',b')) \geq C_{\varepsilon,F} \max(|a'|,|b'|)^{\deg(F)-2-\varepsilon}. \tag{2.27}$$

Or, d'après (2.26), on a $\mathrm{rad}(F(a',b')) \leq |d'c|$. Par ailleurs, il existe une constante M_F ne dépendant que de F telle que

$$\max(|a'|,|b'|)^{\deg(F)} \geq M_F |d'c^p|.$$

On déduit alors de (2.27) l'inégalité suivante

$$|d'c| \geq C_{\varepsilon,F} \left(M_F |d'c^p|\right)^{\alpha}, \quad \text{où } \alpha = 1 - \frac{2+\varepsilon}{\deg(F)}.$$

Supposons $\varepsilon < 1$. On a alors $0 < \alpha < 1$ et

$$|c|^{\alpha p - 1} \leq \frac{|d'|^{1-\alpha}}{C_{\varepsilon,F} M_F^{\alpha}}.$$

Pour p suffisamment grand, cela implique $c = \pm 1$. C'est le résultat voulu.

2.5 Annexe B – La conjecture *abc* implique la conjecture de Frey-Mazur

A. Kraus a montré que la conjecture de Frey et Mazur est une conséquence d'une inégalité conjecturale de Szpiro entre le conducteur et le discriminant minimal d'une courbe elliptique[2]. Rappelons-en l'énoncé ici (*c.f.* [Oes88, Szp90]).

Conjecture 2.35 (Szpiro) *Pour tout ε réel > 0, il existe une constante $C(\varepsilon)$ telle que pour toute courbe elliptique E définie sur $\mathbf{Q}$ de conducteur N et de discriminant minimal Δ, on a*

$$|\Delta| < C(\varepsilon) N^{6+\varepsilon}. \tag{2.28}$$

L'objet de cette annexe est de montrer qu'une version *effective* de la conjecture de Szpiro implique une version *effective* de la conjecture de Frey - Mazur. Plus précisément, on montre le résulat suivant.

Proposition 2.36 *Soit E une courbe elliptique définie sur $\mathbf{Q}$ de conducteur N. Supposons que la conjecture de Szpiro soit vérifiée. Alors, la conjecture de Frey - Mazur l'est également et, si $p \in \mathcal{F}_E$, on a de plus :*

$$p \leq \max\left(\log_2(C(\varepsilon)) + (6+\varepsilon)(1+\log_2 N), 2.6N\sqrt{1+\log\log N}\right).$$

[2]Ce résultat figure sous forme de notes non publiées, dans les Comptes - Rendus du Séminaire de Théorie des Nombres de Caen (exposé XVIII, année 1989 - 1990, *c.f.* [Bil08a, App.B])

La démonstration présentée ici est celle donnée dans [Bil08a, App.B] où l'on a employé le lemme 2.37 à la place du lemme B.2.

Commençons par un lemme général. Soient E et E' deux courbes elliptiques définies sur $\mathbf{Q}$ de *même conducteur* N. Notons S l'ensemble des nombres premiers ℓ en lesquels E (ou E') a réduction multiplicative et $a_\ell \neq a'_\ell$. Suivant [Del85, C.p.253], on définit alors l'entier

$$N(S) = N \prod_{\ell \in S} \ell$$

et pour $n \geq 1$, la fonction multiplicative

$$\mu(n) = \frac{n}{6} \prod_{\ell | n} \left(1 + \frac{1}{\ell}\right).$$

Lemme 2.37 *Supposons que les modules galoisiens $E[p](\overline{\mathbf{Q}})$ et $E'[p](\overline{\mathbf{Q}})$ soient isomorphes pour un nombre premier $p \geq 4\sqrt{\mu(N(S))}$. Alors, les courbes E et E' sont isogènes.*

Démonstration. D'après [KO92, prop.3], l'hypothèse implique que l'on a

$$a_\ell \equiv a'_\ell \pmod{p}, \quad \text{pour tout } \ell \nmid N.$$

Soit ℓ un nombre premier $\leq \mu(N(S))$ n'appartenant pas à S. Si $\ell \mid N$, on a $a_\ell = a'_\ell$ car E et E' ont même réduction en ℓ et $\ell \notin S$. Si $\ell \nmid N$, on a $a_\ell \equiv a'_\ell \pmod{p}$ d'après la congruence ci-dessus.

Dans les deux cas, p divise $|a_\ell - a'_\ell|$. Or, d'après les bornes de Weil, on a

$$|a_\ell - a'_\ell| < 4\sqrt{\ell} \leq 4\sqrt{\mu(N(S))}.$$

Or par hypothèse $p \geq 4\sqrt{\mu(N(S))}$, d'où $a_\ell = a'_\ell$. Par ailleurs d'après [Del85, C. p. 253], cela implique que l'on a $a_\ell = a'_\ell$ pour *tout* nombre premier ℓ. On conclut alors avec le théorème de Faltings ([Fal86, §5,cor.2]).

Démontrons à présent la proposition 2.36. Soient E une courbe elliptique définie sur $\mathbf{Q}$ de conducteur N et discriminant minimal Δ. Soit $p > 7$ un nombre premier *de bonne réduction* appartenant à $\mathcal{F}_E$, c'est-à-dire pour lequel il existe une courbe elliptique $E^{(p)}$ définie sur $\mathbf{Q}$, non isogène à E sur $\mathbf{Q}$, telle que les représentations ρ_p^E et $\rho_p^{E^{(p)}}$ soient isomorphes. D'après [Kra97a, p.28], si $p > \log_2|\Delta|$, on a

$$N\left(\rho_p^E\right) = N, \tag{2.29}$$

où $N\left(\rho_p^E\right)$ est le conducteur de la représentation ρ_p^E donnant l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur la p-torsion de E (c'est la partie première à p du conducteur d'Artin de ρ_p^E, *c.f.* [Ser87, §1]). Les représentations ρ_p^E et $\rho_p^{E^{(p)}}$ étant isomorphes, on a, en particulier,

$$N\left(\rho_p^E\right) = N\left(\rho_p^{E^{(p)}}\right). \tag{2.30}$$

On en déduit que N divise $N_{E^{(p)}}$. On écrit

$$N_{E^{(p)}} = N \cdot u_p. \tag{2.31}$$

Montrons alors que u_p^p divise le discriminant minimal $\Delta_{E^{(p)}}$ de $E^{(p)}$.

On considère pour cela un nombre premier $\ell \neq p$. Alors

$$v_\ell\left(N\left(\rho_p^{E^{(p)}}\right)\right) = v_\ell\left(N_{E^{(p)}}\right)$$

sauf si $E^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{E^{(p)}})$ ([Kra97a, p.28]). Autrement dit, si ℓ divise u_p, alors, d'après les égalités (2.29) et (2.30) et la remarque ci-dessus, $E^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{E^{(p)}})$. En particulier, $v_\ell(u_p) = 1$.

La courbe E a bonne réduction en p par hypothèse. Donc le poids de ρ_p^E est 2 ([Ser87]). On en déduit que la représentation $\rho_p^{E^{(p)}}$ est également de poids 2 et que l'on est dans l'un des cas suivants :

1. la courbe $E^{(p)}$ a bonne réduction en p ;
2. la courbe $E^{(p)}$ a mauvaise réduction multiplicative en p et l'exposant de p dans $\Delta_{E^{(p)}}$ est multiple de p ;
3. la courbe $E^{(p)}$ a mauvaise réduction additive en p.

Or d'après [Kra97a, p.6], si $E^{(p)}$ a mauvaise réduction additive en p et si $\rho_p^{E^{(p)}}$ est de poids 2, alors $p \leq 7$. C'est absurde car on a supposé $p > 7$. Le cas 3 ne peut donc pas se produire.

On en déduit donc, comme annoncé, que u_p^p divise $\Delta_{E^{(p)}}$. On applique à présent l'inégalité de Szpiro à la courbe $E^{(p)}$. Soit $\varepsilon > 0$, on a :

$$|\Delta_{E^{(p)}}| < C(\varepsilon) N_{E^{(p)}}^{6+\varepsilon}.$$

Or d'après l'égalité (2.31) et le fait que u_p^p divise $\Delta_{E^{(p)}}$, on a

$$|u_p|^{p-(6+\varepsilon)} < C(\varepsilon) N^{6+\varepsilon}.$$

Donc si $p > \log_2(C(\varepsilon)) + (6+\varepsilon)(1+\log_2 N)$, alors $u_p = 1$. On en déduit

$$N_{E^{(p)}} = N.$$

D'après le lemme 2.37 appliqué aux courbes E et $E^{(p)}$, on a une contradiction si

$$p \geq 4\sqrt{\mu(N(S))},$$

où S désigne l'ensemble des nombres premiers ℓ où les courbes E et $E^{(p)}$ ont réduction multiplicative et $a_\ell(E) \neq a_\ell(E')$. Comme $N(S)$ divise N^2, on a en particulier une contradiction dès lors que $p \geq 4\sqrt{\mu(N^2)}$. Par ailleurs, d'après [Kra95, (1)], on a

$$4\sqrt{\mu(N^2)} \leq 2.6N\sqrt{1+\log\log N}.$$

Par ailleurs, on a d'une part,

$$\log_2(C(\varepsilon)) + (6+\varepsilon)(1+\log_2 N) > \log_2|\Delta|$$

d'après l'inégalité de Szpiro appliquée à E. D'autre part,

$$2.6N\sqrt{1+\log\log N} > N > 7.$$

Donc, si $p \geq 2.6N\sqrt{1+\log\log N}$, alors $p > 7$ et p ne divise pas N. D'où le résultat.

Deuxième partie

Arithmétique des courbes elliptiques

Chapitre 3

Défaut de semi-stabilité des courbes elliptiques

Ce chapitre reproduit le texte [Bil08b] soumis en juin 2008 à la revue Dissertationes Mathematicae *à l'exception de l'annexe C qui a été ajoutée.*

Introduction

Étant donnés un nombre premier p, une clôture algébrique $\overline{\mathbf{Q}_p}$ de $\mathbf{Q}_p$ et une extension finie K de $\mathbf{Q}_p$ contenue dans $\overline{\mathbf{Q}_p}$, on considère une courbe elliptique E définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier. Il existe alors une plus petite extension L de la clôture non ramifiée K_{nr} de K dans $\overline{\mathbf{Q}_p}$ où E acquiert bonne réduction. Si E_n désigne le groupe des points de n-torsion de E, on a $L = K_{nr}(E_n)$ pour tout entier $n \geq 3$ non divisible par p ([ST68, 2.cor.3.]). Le groupe $\Phi = \mathrm{Gal}(L/K_{nr})$ est connu dans le cas où $p \geq 3$ ([Kra90]). Lorsque $p = 2$, il est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe à un groupe quaternionien, soit d'ordre 24 et isomorphe à $\mathrm{SL}_2(\mathbf{F}_3)$. La détermination précise du groupe Φ lorsque $p = 2$ n'a été menée que dans deux cas : par A. Kraus pour $K = \mathbf{Q}_2$ ([Kra90]) et par É. Cali pour toutes les extensions finies $K/\mathbf{Q}_2$ non ramifiées ([Cal04]).

Le présent travail a deux objectifs : d'une part, établir en fonction de la valuation de j modulo 12 plusieurs résultats généraux sur le groupe Φ, valables pour toute extension finie $K/\mathbf{Q}_2$ et, d'autre part, le déterminer explicitement en fonction des coefficients d'une équation de Weierstrass de E dans le cas des extensions quadratiques ramifiées de $\mathbf{Q}_2$. Combiné avec les travaux de Cali et Kraus, ce dernier résultat achève le calcul du groupe Φ pour toutes les extensions de $\mathbf{Q}_2$ de degré ≤ 2.

3.1 Énoncés des résultats

Soient K une extension finie de $\mathbf{Q}_2$ d'indice de ramification e, π une uniformisante de K et v la valuation de K normalisée par $v(\pi) = 1$. Soit E une courbe elliptique définie sur K d'invariant modulaire j ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire est de valuation ≥ 0.

L'article se compose de deux parties. Dans la première on établit l'ordre du groupe Φ pour certaines valeurs de la congruence de $v(j)$ modulo 12. Les seuls résultats généraux connus sont les suivants ([Kra90, th.2]) :

1. si $v(j) = 0$, alors on a $|\Phi| = 2$.
2. supposons $v(j) \geq 12e$.
   (a) Si $v(j)$ est divisible par 3, on a $|\Phi| = 2$;
   (b) Si $v(j)$ n'est pas divisible par 3, on a $|\Phi| = 3$ si le type de Néron de E est IV ou IV^* et $|\Phi| = 6$ sinon.

En particulier, aucun résultat n'a été démontré si l'on a $0 < v(j) < 12e$. Dans ce cas, on obtient l'énoncé suivant.

Théorème 3.1 *Supposons* $0 < v(j) < 12e$.

1. *Supposons* $v(j) \equiv \pm 3 \pmod{12}$, *alors* $|\Phi| = 8$.
2. *Supposons* $v(j) \equiv \pm 1 \pmod{12}$ *ou* $v(j) \equiv \pm 5 \pmod{12}$, *alors* $|\Phi| = 24$.
3. *Supposons* $v(j) \equiv \pm 2 \pmod{12}$ *et* $|6e - v(j)| > 2e$, *alors* $|\Phi| = 24$.

Dans tous les autres cas, la valuation de j ne suffit pas à déterminer l'ordre du groupe Φ (*cf.* [Cal04] et le Théorème 3.2 ci-dessous).

Dans la seconde partie de ce travail, on détermine le groupe Φ lorsque K est une extension quadratique ramifiée de $\mathbf{Q}_2$. Il y a exactement six telles extensions que l'on regroupe en deux ensembles de la façon suivante :

$$\Omega_1 = \{\mathbf{Q}_2(\sqrt{-1}), \mathbf{Q}_2(\sqrt{3})\}$$

et

$$\Omega_2 = \{\mathbf{Q}_2(\sqrt{2}), \mathbf{Q}_2(\sqrt{-2}), \mathbf{Q}_2(\sqrt{6}), \mathbf{Q}_2(\sqrt{-6})\}.$$

On suppose E donnée par une équation de Weierstrass entière, non nécessairement minimale, et dont (c_4, c_6, Δ) sont les invariants standard ([Tat75]) qui lui sont associés. On a $j = c_4^3/\Delta$. Dans le cas où jc_6 est non nul, on pose

$$c_4 = \pi^{v(c_4)} c_4', \quad c_6 = \pi^{v(c_6)} c_6',$$

$$\Delta = \pi^{v(\Delta)} \Delta' \quad \text{et} \quad j' = c_4'^3/\Delta'.$$

On désigne par (C1), (C1'), (C2), et (C3) les conditions suivantes :

$$\Delta' \equiv 1 + \pi \pmod 2 \tag{C1}$$

$$c_4' \equiv 1 + \pi \pmod 2 \tag{C1'}$$

$$j' \equiv 1 + \pi^2 \pmod{\pi^3} \tag{C2}$$

$$c_4' \equiv 1 + \pi^2 \pmod 4 \quad \text{ou} \quad c_4' \equiv 1 + \pi^3 \pmod 4. \tag{C3}$$

Remarques.

1. Les conditions ci-dessus sont indépendantes du modèle choisi pour représenter la courbe E. En particulier, il n'est pas nécessaire qu'il soit minimal.

2. Elles ne dépendent pas non plus du choix de l'uniformisante de K.

Notations. On note ε l'unité de l'anneau des entiers de K définie par

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2.$$

On définit alors les ensembles suivants de couples d'unités de l'anneau des entiers de K :

$$\begin{aligned}\mathcal{L}_1 = \big\{&(-\varepsilon^2+6+\pi^6+\pi^7, -\varepsilon), (-\varepsilon^2+2\pi^4+6+\pi^6+\pi^7, -\varepsilon+\pi^4)\\ &(-\varepsilon^2+6+\pi^6, -\varepsilon+\pi^5), (-\varepsilon^2+2\pi^4+6+\pi^6, -\varepsilon+\pi^4+\pi^5),\\ &(-\varepsilon^2+2\varepsilon\pi^2+6-\pi^4+\pi^6, -\varepsilon+\pi^2), (-\varepsilon^2+2\varepsilon\pi^2+6+\pi^4+\pi^6, -\varepsilon+\pi^2+\pi^4),\\ &(-\varepsilon^2+2\varepsilon\pi^2+6-\pi^4+\pi^6+\pi^7, -\varepsilon+\pi^2+\pi^5), (-\varepsilon^2+2\varepsilon\pi^2+6+\pi^4+\pi^6+\pi^7,\\ &-\varepsilon+\pi^2+\pi^4+\pi^5), (-\varepsilon^2+2\varepsilon\pi^3+6, -\varepsilon+\pi^3), (-\varepsilon^2+2\varepsilon\pi^3+6+2\pi^4,\\ &-\varepsilon+\pi^3+\pi^4), (-\varepsilon^2+2\varepsilon\pi^3+6+\pi^7, -\varepsilon+\pi^3+\pi^5), (-\varepsilon^2+2\varepsilon\pi^3+6+2\pi^4+\pi^7,\\ &-\varepsilon+\pi^3+\pi^4+\pi^5), (-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6, -\varepsilon+\pi^2+\pi^3),\\ &(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6, -\varepsilon+\pi^2+\pi^3+\pi^4),\\ &(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6+\pi^7, -\varepsilon+\pi^2+\pi^3+\pi^5),\\ &(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6+\pi^7, -\varepsilon+\pi^2+\pi^3+\pi^4+\pi^5)\big\};\end{aligned}$$

$$\begin{aligned}\mathcal{L}_2 = \Big\{&\left(-1, \frac{2}{\pi^2}\right), \left(-1+\pi^2+\pi^3, \frac{2}{\pi^2}\right), \left(1, \frac{2}{\pi^2}+\pi^2\right),\\ &\left(1+\pi^2+\pi^3, \frac{2}{\pi^2}+\pi^2\right), \left(-1+\pi^3, \frac{2}{\pi^2}+\pi^3\right), \left(-1+\pi^2, \frac{2}{\pi^2}+\pi^3\right),\\ &\left(1+\pi^3, \frac{2}{\pi^2}+\pi^2+\pi^3\right), \left(1+\pi^2, \frac{2}{\pi^2}+\pi^2+\pi^3\right)\Big\}.\end{aligned}$$

Théorème 3.2 *On suppose que l'extension $K/\mathbf{Q}_2$ est quadratique ramifiée. On est dans l'un des cas suivants.*

1. *Si $v(j) = 0$, on a $|\Phi| = 2$.*
2. *Si $v(j) \in \{1, 2, 5, 7, 10, 11, 13, 14, 17, 19, 22, 23\}$, on a $|\Phi| = 24$.*
3. *Si $v(j) \in \{3, 9, 15, 21\}$, on a $|\Phi| = 8$.*
4. *Supposons $v(j) = 4$.*
   (a) *Supposons que la condition* (C1) *soit satisfaite.*
   On a $|\Phi| = 3$ si les conditions suivantes sont satisfaites :
      i. *on a $v(\Delta) \equiv 8 \pmod{12}$;*
      ii. *Si $K \in \Omega_1$, on a $c_6' \equiv 1 + \pi^2 \pmod 4$ ou $c_6' \equiv 1 + \pi^3 \pmod 4$;*
      iii. *Si $K \in \Omega_2$, on a $c_6' \equiv 1 \pmod 4$ ou $c_6' \equiv 1 + \pi^2 + \pi^3 \pmod 4$.*

   On a $|\Phi| = 6$ sinon.
   (b) *Si la condition* (C1) *n'est pas satisfaite, on a $|\Phi| = 24$.*

5. *Supposons* $v(j) = 6$. *On a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1) est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

6. *Supposons* $v(j) = 8$.
   (a) *Supposons que la condition* (C2) *soit satisfaite.*
   On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*
      i. *on a* $v(\Delta) \equiv 4 \pmod{12}$ *;*
      ii. *il existe* $(a, b) \in \mathcal{L}_1$ *tel que* $c_4' \equiv a \pmod{\pi^8}$ *et* $c_6' \equiv b \pmod{\pi^6}$.
   On a $|\Phi| = 6$ *sinon.*
   (b) *Si la condition* (C2) *n'est pas satisfaite, on a* $|\Phi| = 24$.
7. *Supposons* $v(j) = 12$.
   (a) *Si* $2v(c_6) = 3v(c_4) + 1$, *on a* $|\Phi| = 8$.
   (b) *Si* $2v(c_6) = 3v(c_4) + 2$.
      i. *Si* $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1') est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

      ii. *Si* $K \in \Omega_2$, *on a*

$$|\Phi| = \begin{cases} 8 & \text{si la condition (C1') est satisfaite,} \\ 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

   (c) *Si* $2v(c_6) = 3v(c_4) + 3$, *on a*

$$|\Phi| = \begin{cases} 8 & \text{si } K \in \Omega_1, \\ 4 & \text{si } K \in \Omega_2. \end{cases}$$

   (d) *Si* $2v(c_6) - 3v(c_4) \geq 4$.
      i. *Si* $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite et } v(c_4) \text{ est pair,} \\ 4 & \text{sinon.} \end{cases}$$

      ii. *Si* $K \in \Omega_2$, *on a* $|\Phi| = 8$.
8. *Supposons* $v(j) = 16$.
   (a) *Supposons que la condition* (C2) *soit satisfaite.*
   On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*
      i. *on a* $v(\Delta) \equiv 8 \pmod{12}$ *;*
      ii. *il existe* $(a, b) \in \mathcal{L}_2$ *tel que* $c_4' \equiv a \pmod{4}$ *et* $c_6' \equiv b \pmod{4}$.
   On a $|\Phi| = 6$ *sinon.*
   (b) *Si la condition* (C2) *n'est pas satisfaite, on a* $|\Phi| = 24$.

9. *Supposons* $v(j) = 18$. *On a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1') est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

10. *Supposons* $v(j) = 20$.
    (a) *Supposons que la condition* (C1') *soit satisfaite.*
    On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*
    i. *on a* $v(\Delta) \equiv 4 \pmod{12}$;
    ii. *on a* $c_6' \equiv \frac{\pi^2}{2} + 2 \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + \pi^3 \pmod 4$.
    On a $|\Phi| = 6$ *sinon.*
    (b) *Si la condition* (C1') *n'est pas satisfaite, on a* $|\Phi| = 24$.
11. *Supposons* $v(j) \geq 24$.
    (a) *Si* 3 *divise* $v(\Delta)$, *on a* $|\Phi| = 2$.
    (b) *Supposons que* 3 *ne divise pas* $v(\Delta)$.
    On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*
    i. *on a* $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$;
    ii. *on a* $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.
    On a $|\Phi| = 6$ *sinon.*

Dans l'Appendice 3.4, on montre que chacun des cas ci-dessus se réalise.

3.2 Le cas des extensions quelconques

3.2.1 Lemmes sur les carrés

On reprend les notations de la section 3.1. Il existe une unique extension quadratique non ramifiée de K dans $\overline{K}$. On la note N. Lorsque l'extension $K/\mathbf{Q}_2$ est totalement ramifiée, le corps résiduel de N est de cardinal 4 et un système de représentants est $\mu_3 \cup \{0\}$, où μ_3 est l'ensemble des racines cubiques de l'unité. On note $\mathcal{O}_K$ (resp. $\mathcal{O}_N$) l'anneau des entiers de K (resp. de N) et $\mathcal{U}_K$ (resp. $\mathcal{U}_N$) ses unités.

Par commodité, on rappelle le résultat suivant ([Kra90, lem.7]).

Lemme 3.3 *Soit* x *un élément de* $\mathcal{U}_K$ *congru à* 1 *modulo* $4\mathcal{O}_K$. *Alors,* x *est un carré dans* K_{nr}.

On en déduit le résultat suivant.

Lemme 3.4 *Soit* x *un élément de* $\mathcal{U}_K$. *Alors,* x *est un carré dans* K_{nr} *si et seulement si il existe un élément* y *de* $\mathcal{U}_N$ *tel que*

$$x \equiv y^2 \pmod{4\mathcal{O}_N}.$$

Démonstration. La condition est nécessaire car si x est un carré dans K_{nr}, c'est un carré dans une extension quadratique non ramifiée de K, donc dans N. Réciproquement, s'il existe un élément y de N tel que $x \equiv y^2 \pmod{4\mathcal{O}_N}$, alors, d'après le lemme 3.3, x est un carré dans la clôture non ramifiée de N dans $\overline{K}$. Or $N_{nr} = K_{nr}$ car N/K est non ramifiée. D'où le lemme.

Lorsque l'extension $K/\mathbf{Q}_2$ est totalement ramifiée, on a le résultat plus précis suivant.

Lemme 3.5 *Supposons l'extension $K/\mathbf{Q}_2$ totalement ramifiée. Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si il existe un élément $y \in \mathcal{U}_K$ tel que $x \equiv y^2 \pmod{4\mathcal{O}_K}$. Autrement dit, x est un carré dans K_{nr} si et seulement si il existe des éléments $a_0, a_1, \ldots, a_{e-1}$ tels que les deux conditions suivantes soient satisfaites :*

1. *on a $a_0 = 1$ et $a_j = 0$ ou 1 pour $1 \leq j \leq e-1$;*
2. *on a*
$$x \equiv \left(a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}\right)^2 \pmod{4\mathcal{O}_K}. \tag{3.1}$$

Démonstration. La condition est suffisante d'après le lemme précédent.

Réciproquement, supposons que x soit un carré dans K_{nr}. Il existe alors y dans $\mathcal{O}_N$ tel que $x = y^2$. On choisit comme système de représentants du corps résiduel de N l'ensemble μ_3 des racines cubiques de l'unité. On écrit le développement de Hensel de y modulo 2 :

$$y \equiv a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1} \pmod{2\mathcal{O}_N}, \quad \text{où } a_j \in \mu_3 \cup \{0\}.$$

Soit i un entier ≥ 0 et $P(i)$ la proposition de récurrence suivante :

$$\text{« } a_0, \ldots, a_i = 0 \text{ ou } 1 \text{ ».}$$

Montrons $P(0)$. L'extension $K/\mathbf{Q}_2$ étant totalement ramifiée, x est congru à 1 modulo $\pi\mathcal{O}_K$, d'où $y^2 \equiv 1 \pmod{\pi\mathcal{O}_K}$. Or π est une uniformisante de N, donc $\pi\mathcal{O}_N$ est un idéal premier de $\mathcal{O}_N$. On en déduit $y \equiv \pm 1 \pmod{\pi\mathcal{O}_N}$. Puis, comme $-1 \equiv 1 \pmod{\pi}$, il vient $y \equiv 1 \pmod{\pi\mathcal{O}_N}$. Cela démontre $P(0)$ et on a $a_0 = 1$. Si $e = 1$, cela démontre le résultat.

Supposons $e > 1$. Soit $i \geq 0$ tel que $i < e-1$ et $P(i)$ vraie. Montrons $P(i+1)$. Posons

$$z = \frac{1}{\pi^{i+1}}\left(y - (1 + a_1\pi + \cdots + a_i\pi^i)\right).$$

L'élément z est dans $\mathcal{O}_N$. Calculons $z^2 \pmod{\pi\mathcal{O}_N}$ de deux façons différentes.

D'une part, on a

$$z^2 = \frac{1}{\pi^{2(i+1)}}\left(y^2 - 2y(1 + a_1\pi + \cdots + a_i\pi^i) + (1 + a_1\pi + \cdots + a_i\pi^i)^2\right).$$

Or

$$2y(1 + a_1\pi + \cdots + a_i\pi^i) \equiv 2(1 + a_1\pi + \cdots + a_i\pi^i)^2 \pmod{\pi^{e+i+1}\mathcal{O}_N}.$$

Comme $x = y^2$, on en déduit donc,

$$z^2 \equiv \frac{1}{\pi^{2(i+1)}}\left(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2\right) \pmod{\pi^{e-1-i}\mathcal{O}_N}.$$

Posons

$$\alpha = \frac{1}{\pi^{2(i+1)}}\Big(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2\Big).$$

Alors, par hypothèse de récurrence, $\alpha \in \mathcal{O}_N \cap K = \mathcal{O}_K$ et on a, en particulier,

$$\alpha \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

On en déduit alors

$$z^2 \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

D'autre part, on a

$$z \equiv a_{i+1} \pmod{\pi\mathcal{O}_N}, \quad \text{puis } z^2 \equiv a_{i+1}^2 \pmod{\pi\mathcal{O}_N}.$$

On en déduit $a_{i+1} = 0$ ou 1. D'où le résultat par récurrence. On a donc, $x \equiv (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2 \pmod{4\mathcal{O}_N}$ avec $a_1, \ldots, a_{e-1} = 0$ ou 1. D'où

$$\frac{1}{4}\left(x - (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2\right) \in \mathcal{O}_N \cap K = \mathcal{O}_K.$$

D'où la congruence annoncée.

Lemme 3.6 *Soit x un élément de K_{nr} de valuation 0. Alors, toutes les racines cubiques de x dans $\overline{K}$ sont dans K_{nr}.*

Démonstration. L'élément x est une unité des entiers de $K(x)$. Elle s'écrit en particulier, $x = \xi \cdot b$, où ξ est une racine de l'unité d'ordre impair et b une unité principale des entiers de $K(x)$, i.e. $b \equiv 1 \pmod{\pi\mathcal{O}_{K(x)}}$. Or, ξ est un cube dans K_{nr} et le lemme de Hensel appliqué au polynôme $X^3 - b$ de $\mathcal{O}_{K(x)}[X]$ montre qu'il en va de même pour b. D'où le résultat.

On rappelle que e désigne l'indice de ramification de l'extension $K/\mathbf{Q}_2$.

Lemme 3.7 *Soient K'/K_{nr} une extension finie de degré n impair, x et y deux éléments de K' de valuation ≥ 0 et ρ un rationnel positif. On suppose que les conditions suivantes sont satisfaites.*

1. *$v(x - y) = \rho$;*
2. *$\rho = r/s$, avec r et s entiers premiers entre eux et r impair ;*
3. *$\rho \leq 2e$.*

Alors, l'un au-moins des éléments x et y n'est pas un carré dans K'.

Démonstration. Supposons que $x = a^2$ et $y = b^2$ soient des carrés dans K'. On a $v(2b) = e + v(b) = e + v(y)/2 \geq \rho/2$ par hypothèse.

Supposons $v(a - b) < \rho/2$. Alors, d'après l'égalité $a + b = a - b + 2b$, on en déduit $v(a + b) = v(a - b) < \rho/2$. Or, c'est absurde car $v(a - b) + v(a + b) = v(a^2 - b^2) = \rho$. On a donc $v(a - b) \geq \rho/2$ et de même, $v(a + b) \geq \rho/2$. D'où, $v(a - b) = v(a + b) = \rho/2$. Mais, r et n étant impairs, $\rho/2 \notin v(K') \subset \frac{1}{n}\mathbf{Z}$. D'où une contradiction et le lemme.

3.2.2 La courbe $\widetilde{E}$

On reprend les notations de la section 3.1. En particulier, e désigne l'indice de ramification de $K/\mathbf{Q}_2$ et on note encore v le prolongement de la valuation normalisée v de K à une clôture algébrique $\overline{K}$ de K . On choisit une racine cubique $\Delta^{1/3}$ de Δ dans $\overline{K}$. On note M l'extension de K_{nr} engendrée par $\Delta^{1/3}$. D'après le lemme 3.6, si $v(\Delta)$ est divisible par 3, alors $\Delta^{1/3}$ est dans K_{nr}, i.e. l'extension M/K_{nr} est triviale. Réciproquement, si $\Delta^{1/3}$ est dans K_{nr}, alors $v(\Delta)$ est divisible par 3 car $v(K_{nr}) \subset \mathbf{Z}$.

On pose, pour t dans l'ensemble μ_3 des racines cubiques de l'unité :

$$A_t = c_4 - 12t\Delta^{1/3} \quad \text{et} \quad B_t = c_4^2 + 12tc_4\Delta^{1/3} + (12t\Delta^{1/3})^2.$$

Lorsque $t = 1$, on retrouve les éléments $A_1 = A$ et $B_1 = B$ de [Kra90, th.3]. On a également $A_tB_t = c_6^2$. De plus, d'après le lemme 3.6, A_t et B_t sont dans K_{nr} si et seulement si 3 divise $v(\Delta)$, i.e. si et seulement si 3 divise $v(j)$. On désigne par $j^{1/3}$ la racine cubique de j dans $\overline{K}$ définie par l'égalité

$$j^{1/3} = c_4/\Delta^{1/3}.$$

On fait l'hypothèse $v(j) > 6e$. L'équation suivante définit alors un modèle entier d'une courbe elliptique, notée $\widetilde{E}$, sur K :

$$y^2 + 2xy = x^3 + \frac{j}{3(j-1728)}x + \frac{j}{3^3(j-1728)}. \tag{3.2}$$

Les coefficients standard $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ de $\widetilde{E}$ sont donnés par les égalités suivantes :

$$\widetilde{c_4} = -2^4\frac{1728}{j-1728} = -2^{10}\cdot 3^3\frac{\Delta}{c_6^2}, \quad \widetilde{c_6} = 2^6\frac{1728}{j-1728} = 2^{12}\cdot 3^3\frac{\Delta}{c_6^2} \tag{3.3}$$

et

$$\widetilde{\Delta} = -2^{12}\frac{1728j}{(j-1728)^3} = -2^{18}\cdot 3^3\frac{c_4^3\Delta^2}{c_6^6}. \tag{3.4}$$

On vérifie que l'on a $v(\widetilde{\Delta}) = v(j)$. De plus, on a $\widetilde{j} = \widetilde{c_4}^3/\widetilde{\Delta} = 1728^2/j$, d'où en particulier, $v(\widetilde{j}) = 12e - v(j)$.

On choisit de noter $\widetilde{\Delta}^{1/3}$ la racine cubique de $\widetilde{\Delta}$ définie par l'égalité :

$$\widetilde{\Delta}^{1/3} = -2^6\cdot 3\frac{j^{1/3}}{j-1728} = -2^6\cdot 3\frac{c_4\Delta^{2/3}}{c_6^2}.$$

Pour $t \in \mu_3$, on définit, comme pour E ci-dessus, le coefficient

$$\widetilde{B}_t = \widetilde{c_4}^2 + 12t\widetilde{c_4}\widetilde{\Delta}^{1/3} + (12t\widetilde{\Delta}^{1/3})^2.$$

À nouveau, $\widetilde{B}_t$ est dans K_{nr} si et seulement si 3 divise $v(j)$. Posons à présent

$$w_t = 2^4\cdot 3\cdot t^2\frac{\Delta^{1/3}}{c_6}.$$

Proposition 3.8 *On est dans l'un des cas suivants :*

1. *supposons $v(j)$ divisible par 3, alors w_t appartient à K_{nr} ;*

2. *supposons $v(j)$ non divisible par 3, alors w_t n'appartient pas à K_{nr} et w_t appartient à M qui est l'unique extension de degré 3 de K_{nr}.*

De plus, on a, pour $t \in \mu_3$,

$$\widetilde{B}_t = w_t^4 B_{t^2}.$$

Démonstration. Les deux premières assertions résultent du lemme 3.6. On a

$$12 \cdot \frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} = \frac{1}{12} \cdot \frac{c_4}{\Delta^{1/3}}.$$

D'où

$$\frac{\widetilde{B}_t}{\widetilde{c_4}^2} = 1 + 12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} + \left(12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}}\right)^2 = 1 + \frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}} + \left(\frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}}\right)^2$$
$$= \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2 \left(1 + 12t^2\frac{\Delta^{1/3}}{c_4} + \left(12t^2\frac{\Delta^{1/3}}{c_4}\right)^2\right) = \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2 \cdot \frac{B_{t^2}}{c_4^2}.$$

D'où, comme $\widetilde{c_4} = -2^{10} \cdot 3^3\Delta/c_6^2$, on a

$$\widetilde{B}_t = 2^{16} \cdot 3^4 \cdot t^2\frac{\Delta^{4/3}}{c_6^4}B_{t^2} = w_t^4 B_{t^2}$$

et la proposition.

On note, comme $\widetilde{j} \neq 0$, $\widetilde{c_4} = \pi^{v(\widetilde{c_4})}\widetilde{c_4}'$, $\widetilde{\Delta} = \pi^{v(\widetilde{\Delta})}\widetilde{\Delta}'$ et $\widetilde{j} = \pi^{v(\widetilde{j})}\widetilde{j}'$. On vérifie alors d'après les formules (3.3) et (3.4) que l'on a le résultat suivant.

Lemme 3.9 *On a*

$$\widetilde{\Delta}' = -3^3 \cdot \left(\frac{2}{\pi^e}\right)^{18} \frac{c_4'^3\Delta'^2}{c_6'^6} \quad \textit{et} \quad j'\widetilde{j}' = 3^6 \cdot \left(\frac{2}{\pi^e}\right)^{12}.$$

3.2.3 Démonstration du théorème 3.1

On suppose que l'on a $0 < v(j) < 12e$. On reprend les notations introduites à la section 3.2.2 et on choisit une racine carrée $B^{1/2}$ de B dans $\overline{K}$. On pose alors :

$$C = 2\left(c_4 + 6\Delta^{1/3} + B^{1/2}\right).$$

La proposition suivante est à peu de choses près [Cal04, prop.1].

Proposition 3.10 *Supposons $c_6 \neq 0$ et $v(j) \equiv 0 \pmod 3$. Alors, si pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}, on a $|\Phi| = 8$.*

Démonstration. D'après [Kra90, th.3], il s'agit de montrer que C n'est pas un carré dans $K_{nr}(B^{1/2})$. On a $A_tB_t = c_6^2$ qui est non nul par hypothèse. Donc A_t est un carré dans K_{nr} si et seulement si B_t l'est. De plus, on a $c_4 \neq 0$ (car B_t n'est pas un carré dans K_{nr}). Posons

$$\nu = 1 + \frac{B^{1/2}}{c_4}.$$

Alors, $(1, \nu)$ est une base de $K_{nr}(B^{1/2})$ sur K_{nr}. Supposons que C soit un carré dans $K_{nr}(B^{1/2})$. Il existe deux éléments a et b de K_{nr} tels que

$$C = c_4(12j^{-1/3} + 2\nu) = (a + b\nu)^2. \tag{3.5}$$

Or, on vérifie que l'on a $\nu^2 = 2\nu + 12j^{-1/3} + 144j^{-2/3}$. Mais, $j^{1/3} \in K_{nr}$ car $v(j) \equiv 0 \pmod 3$, donc d'après (3.5), il vient

$$\begin{cases} c_4 = b(a+b) \\ 12c_4 j^{-1/3} = a^2 + b^2(12j^{-1/3} + 144j^{-2/3}), \end{cases}$$

puis, $a^2 - 12abj^{-1/3} + 144b^2j^{-2/3} = 0$. Autrement dit, il existe $t \neq 1$ dans μ_3 tel que $a = -12tbj^{-1/3}$. D'où, $c_4 = b^2(1 - 12tj^{-1/3})$. Or, $A_t = c_4(1 - 12tj^{-1/3})$, donc $A_t = b^2(1 - 12tj^{-1/3})^2$ est un carré dans K_{nr} et B_t l'est aussi et ceci contredit l'hypothèse. D'où le résultat.

Démonstration de l'assertion 1

On fait l'hypothèse $v(j) \equiv \pm 3 \pmod{12}$. On a en particulier, $v(j) \equiv 0 \pmod 3$, donc $j^{1/3} \in K_{nr}$.

Supposons dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est impair et vérifie l'inégalité $0 < v(12j^{-1/3}) \leq 2e$. Alors, pour $t \in \mu_3$,

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + (12tj^{-1/3})^2$$

est une unité de K_{nr} et

$$v\left(\frac{B_t}{c_4^2} - 1\right) = v(12tj^{-1/3}) = 2e - \frac{v(j)}{3}.$$

D'après le lemme 3.7 appliqué à $K' = K_{nr}$, $x = B_t/c_4^2$, $y = 1$ et $\rho = 2e - v(j)/3$, B_t n'est pas un carré dans K_{nr}. D'après la proposition 3.10, on a donc $|\Phi| = 8$.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, pour tout $t \in \mu_3$, $\widetilde{B}_t$ n'est pas un carré dans K_{nr}. Or, d'après la proposition 3.8, cela vaut aussi pour B_{t^2}. Ainsi, pour tout t dans μ_3, B_{t^2} n'est pas un carré dans K_{nr}. D'après la proposition 3.10, cela implique $|\Phi| = 8$.

Cela démontre l'assertion 1 du théorème 3.1.

Démonstration de l'assertion 2

On fait l'hypothèse $v(j) \equiv \pm 1 \pmod{12}$ ou $v(j) \equiv \pm 5 \pmod{12}$. En particulier, $v(j)$ est impair et n'est pas divisible par 3.

Supposons dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est > 0. On a alors,

$$v\left(\frac{B}{c_4^2} - 1\right) = v(12j^{-1/3}) = 2e - \frac{v(j)}{3} = \frac{6e - v(j)}{3} \leq 2e.$$

Or, par hypothèse, $6e - v(j)$ est impair et n'est pas divisible par 3. D'après le lemme 3.7 appliqué à $K' = K_{nr}(\Delta^{1/3}) = M$, $x = B/c_4^2$, $y = 1$ et $\rho = (6e - v(j))/3$, B n'est pas un carré dans M.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, $\widetilde{B}$ n'est pas un carré dans M. Or, d'après la proposition 3.8, cela vaut aussi pour B.

D'après [Kra90, th.3], cela implique $|\Phi| = 24$ et l'assertion 2 du théorème 3.1.

Démonstration de l'assertion 3

On a $v(j) \equiv \pm 2 \pmod{12}$ de sorte que $v(j)$ n'est pas divisible par 3. Supposons tout d'abord $v(j) < 6e$. Alors,

$$\frac{B}{c_4^2} = 1 + 12j^{-1/3} + 144j^{-2/3}$$

est une unité de M. Notons π_0 une racine cubique de π dans $\overline{K}$ et supposons que B soit un carré dans M. Il existe alors a, b et c dans K_{nr} tels que

$$\begin{aligned}\frac{B}{c_4^2} &= (a + b\pi_0 + c\pi_0^2)^2 \\ &= (a^2 + 2bc\pi) + (c^2\pi + 2ab)\pi_0 + (b^2 + 2ac)\pi_0^2. \end{aligned} \tag{3.6}$$

Or, $v(\pi_0) = 1/3$, donc $v(a)$, $v(b\pi_0)$ et $v(c\pi_0^2)$ sont distincts puis, d'après l'égalité

$$0 = v\left(\frac{B}{c_4^2}\right) = 2v(a + b\pi_0 + c\pi_0^2),$$

il vient, $v(a) = 0$, $v(b) \geq 0$ et $v(c) \geq 0$. Posons par ailleurs

$$u = \frac{j^{1/3}}{\pi_0^{v(j)}}.$$

On a $u^3 = j'$ et $v(j') = 0$, donc $u \in K_{nr}$ en vertu du lemme 3.6.

On distingue à présent deux cas selon la congruence de $v(j)$ modulo 12.

Supposons $v(j) \equiv 2 \pmod{12}$**.** Écrivons $v(j) = 12k + 2$, $k \geq 0$. On a alors,

$$j^{-1/3} = u^{-1}\pi_0^{-12k-2} = \frac{u^{-1}}{\pi^{4k+1}}\pi_0 \quad \text{et} \quad j^{-2/3} = \frac{u^{-2}}{\pi^{8k+2}}\pi_0^2,$$

puis,

$$\frac{B}{c_4^2} = 1 + 12\frac{u^{-1}}{\pi^{4k+1}}\pi_0 + 144\frac{u^{-2}}{\pi^{8k+2}}\pi_0^2$$

et l'on peut identifier dans (3.6) les coefficients de la décomposition dans la base $(1, \pi_0, \pi_0^2)$. Il vient en particulier (comme $u \in K_{nr}$) :

$$\begin{cases} c^2\pi + 2ab = 12 \cdot u^{-1}/\pi^{4k+1} \\ b^2 + 2ac = 144 \cdot u^{-2}/\pi^{8k+2}. \end{cases} \tag{3.7}$$

Supposons $2v(b) \geq 4e - 8k - 2 = v(144u^{-2}/\pi^{8k+2})$. Alors, d'après (3.7), on a $v(2ac) = e + v(c) \geq 4e - 8k - 2$. Puis, comme $e + v(b) > 2e - 4k - 1$, on a $v(c^2\pi) = 2v(c) + 1 = 2e - 4k - 1$, i.e. $v(c) = e - 2k - 1$. Or,

$$e - 2k - 1 \geq 3e - 8k - 2 \Longrightarrow v(j) \geq 4e.$$

Si $v(j) < 4e$, on a une contradiction et l'hypothèse $2v(b) \geq v(144u^{-2}/\pi^{8k+2})$ est absurde.

Supposons que tel soit le cas, i.e. $v(j) < 4e$. On a alors $2v(b) < 4e - 8k - 2$, puis d'après (3.7), $e + v(c) = 2v(b)$, d'où $2v(c) + 1 = 4v(b) - 2e + 1$. On distingue à présent trois cas.

1. Supposons $2v(c) + 1 = e + v(b)$. Alors, $3(v(b) - e) + 1 = 0$, d'où une contradiction en réduisant cette égalité modulo 3.
2. Supposons $2v(c) + 1 > e + v(b)$, i.e. $4v(b) - 2e + 1 > e + v(b)$. Alors, d'après (3.7), $e + v(b) = 2e - 4k - 1$, i.e. $v(b) = e - 4k - 1$. Or, $4v(b) - 2e + 1 > e + v(b)$ par hypothèse. Donc $v(j) < 0$. C'est une contradiction.
3. Supposons $2v(c) + 1 < e + v(b)$. Alors, d'après (3.7), $2v(c) + 1 = 2e - 4k - 1$, puis $v(c) = e - 2k - 1$. Or, $2v(b) = v(c) + e$, donc $2v(b) = 2e - 2k - 1$. On en déduit une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse B est un carré dans M est absurde si $v(j) \equiv 2 \pmod{12}$ et $v(j) < 4e$.

Supposons $v(j) \equiv -2 \pmod{12}$. Écrivons $v(j) = 12k + 10$, $k \geq 0$. On a alors,

$$j^{-1/3} = u^{-1}\pi_0^{-12k-10} = \frac{u^{-1}}{\pi^{4k+4}}\pi_0^2 \quad \text{et} \quad j^{-2/3} = \frac{u^{-2}}{\pi^{8k+7}}\pi_0,$$

puis,

$$\frac{B}{c_4^2} = 1 + 144\frac{u^{-2}}{\pi^{8k+7}}\pi_0 + 12\frac{u^{-1}}{\pi^{4k+1}}\pi_0^2$$

et l'on peut identifier dans (3.6) les coefficients de la décomposition dans la base $(1, \pi_0, \pi_0^2)$. Il vient en particulier (comme $u \in K_{nr}$) :

$$\begin{cases} c^2\pi + 2ab = 144 \cdot u^{-2}/\pi^{8k+7} \\ b^2 + 2ac = 12 \cdot u^{-1}/\pi^{4k+4}. \end{cases} \tag{3.8}$$

On distingue trois cas.

1. Supposons $2v(b) > 2e - 4k - 4$, i.e. $v(b) > e - 2k - 2$. Alors, d'après (3.8), on a $e + v(c) = 2e - 4k - 4$, i.e. $v(c) = e - 4k - 4$. Donc $2v(c) + 1 = 2e - 8k - 7$, puis $2v(c) + 1 < 4e - 8k - 7 = v(144u^{-2}/\pi^{8k+7})$. Alors, d'après (3.8), $v(2ab) = e + v(b) = 2v(c) + 1 = 2e - 8k - 7$. Autrement dit, $v(b) = e - 8k - 7$, d'où $e - 8k - 7 > e - 2k - 2$. Or cela équivaut à $v(j) < 0$. D'où une contradiction.
2. Supposons $2v(b) < 2e - 4k - 4$, i.e. $v(b) < e - 2k - 2$. Alors, d'après (3.8), on a $e + v(c) = 2v(b)$, puis $2v(c) + 1 = 4v(b) - 2e + 1$. En réduisant en modulo 3, on constate que l'égalité $e + v(b) = 4v(b) - 2e + 1$ est impossible. De plus,

$$2v(c) + 1 = 4v(b) - 2e + 1 > e + v(b) \Longleftrightarrow v(b) > e - \frac{1}{3} \Longleftrightarrow v(b) \geq e,$$

car e et $v(b)$ sont entiers. Or, l'hypothèse faite entraîne $v(b) < e$. On a alors $2v(c) + 1 = 4v(b) - 2e + 1 = 4e - 8k - 7$, puis $2v(b) = 3e - 4k - 4$. Comme $2v(b) < 2e - 4k - 4$, on en déduit $e < 0$. C'est donc une contradiction et l'hypothèse $2v(b) < 2e - 4k - 4$ était absurde.

3. On a donc finalement $2v(b) = 2e - 4k - 4$, i.e. $v(b) = e - 2k - 2$. Donc

$$e + v(b) = 2e - 2k - 2 < 4e - 8k - 7 \Longleftrightarrow v(j) < 4e.$$

Autrement dit, si $v(j) < 4e$, il vient, d'après (3.8), $2v(c) + 1 = e + v(b) = 2e - 2k - 2$. D'où une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse B est un carré dans M est absurde si $v(j) \equiv -2 \pmod{12}$ et $v(j) < 4e$.

Il reste donc à voir que si $v(j) \equiv \pm 2 \pmod{12}$ et $v(j) > 8e$, alors B n'est pas un carré dans M. On considère pour ce faire, la courbe $\widetilde{E}$ d'équation (3.2). On a

$$v(\widetilde{j}) = 12e - v(j) \equiv -v(j) \equiv \pm 2 \pmod{12} \quad \text{et} \quad v(\widetilde{j}) < 4e.$$

Autrement dit, la courbe $\widetilde{E}$ satisfait aux hypothèses précédentes, donc $\widetilde{B}$ n'est pas un carré dans M et B non plus, d'après la proposition 3.8.

D'après [Kra90, th.3], on a donc $|\Phi| = 24$. Cela démontre bien l'assertion 3 du théorème 3.1 et achève sa démonstration.

3.3 Le cas des extensions quadratiques

On reprend les notations ds sections 3.1 et 3.2.1 et l'on suppose l'extension $K/\mathbf{Q}_2$ quadratique ramifiée. Désignons par π_0 une racine cubique de π dans $\overline{K}$. C'est une uniformisante de l'extension $K_{nr}(\pi_0)/K_{nr}$.

3.3.1 Lemmes généraux

Lemme 3.11 *Soit x un élément de $\mathcal{U}_K$. Alors,*

$$x^2 \equiv \begin{cases} 1 \pmod{4\pi} & \text{si } x \equiv 1 \pmod 2 \\ 1 + \pi^2 + \pi^3 \pmod 4 & \text{si } x \equiv 1 + \pi \pmod 2. \end{cases}$$

En particulier, on a $x^2 \equiv 1 \pmod 2$.

Démonstration. Si $x \equiv 1 \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1 + 2a$. Puis $x^2 = 1 + 4a(a+1)$. Or, $a(a+1) \equiv 0 \pmod \pi$, donc $x^2 \equiv 1 \pmod 4$. De même, si $x \equiv 1 + \pi \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1 + \pi + 2a$. Puis $x^2 \equiv 1 + \pi^2 + 2\pi \pmod 4$. Or, 2 est associé à π^2, d'où $2\pi \equiv \pi^3 \pmod 4$ et la congruence annoncée. Dans les deux cas, on a $x^2 \equiv 1 \pmod 2$. D'où le résultat.

Lemme 3.12 *Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si $x \equiv 1$ ou $1 + \pi^2 + \pi^3 \pmod 4$.*

Démonstration. D'après le lemme 3.5, x est un carré dans K_{nr} si et seulement si x est un carré modulo $4\mathcal{O}_K$. On conclut alors avec le lemme précédent.

Lemme 3.13 *Soient x un élément de $\mathcal{U}_K$ congru à 1 modulo 4 et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$. Alors, on a $\sqrt{x} \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$.*

Démonstration. D'après le lemme 3.12, $\sqrt{x} \in K_{nr}$. Supposons $v(\sqrt{x}-1) < 2$. Alors, d'après l'égalité, $\sqrt{x}+1 = \sqrt{x}-1+2$, il vient, $v(\sqrt{x}+1) = v(\sqrt{x}-1) < 2$. Donc $v(x-1) < 4$ ce qui est contraire aux hypothèses. D'où le lemme.

Pour chacune des six extensions quadratiques ramifiées de $\mathbf{Q}_2$, on indique dans le tableau ci-dessous un choix d'uniformisante.

K	$\mathbf{Q}_2(\sqrt{-1})$	$\mathbf{Q}_2(\sqrt{3})$	$\mathbf{Q}_2(\sqrt{2})$	$\mathbf{Q}_2(\sqrt{-2})$	$\mathbf{Q}_2(\sqrt{6})$	$\mathbf{Q}_2(\sqrt{-6})$
π	$1+\sqrt{-1}$	$1+\sqrt{3}$	$\sqrt{2}$	$\sqrt{-2}$	$\sqrt{6}$	$\sqrt{-6}$

Avec ces choix d'uniformisantes, si K est dans Ω_1, on vérifie que l'on a

$$2 \equiv \pi^2 + \pi^3 \pmod 4 \quad \text{et} \quad -1 \equiv 1 + \pi^2 + \pi^3 \pmod 4. \tag{3.9}$$

De même, si K est dans Ω_2, on a

$$2 \equiv \pi^2 \pmod 4 \quad \text{et} \quad -1 \equiv 1 + \pi^2 \pmod 4. \tag{3.10}$$

Remarque. On vérifie que le développement de Hensel de 2 modulo 4 est indépendant du choix de l'uniformisante de K.

On rappelle que l'on a posé

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2. \tag{3.11}$$

Lemme 3.14 *On a*

$$\varepsilon \equiv \begin{cases} 1 \pmod 4 & \text{si } K \in \Omega_1 \\ -1 \equiv 1+\pi^2 \pmod 4 & \text{si } K \in \Omega_2. \end{cases}$$

En particulier, $\varepsilon \equiv 1 \pmod 2$.

Démonstration. D'après les congruences (3.9) et (3.10), on a

$$\frac{2}{\pi^2} \equiv \begin{cases} 1+\pi \pmod 2 & \text{si } K \in \Omega_1 \\ 1 \pmod 2 & \text{si } K \in \Omega_2. \end{cases}$$

D'où le résultat en élevant au carré.

3.3.2 Carrés dans l'extension quadratique non ramifiée de K

Par unicité d'une extension quadratique non ramifiée de K dans $\overline{K}$, on a $N = K(\zeta)$ où ζ est une racine primitive cubique de l'unité dans $\overline{K}$.

Lemme 3.15 *Soit x une unité de l'anneau d'entiers de $K(\zeta)$ congrue modulo 4 à l'un des éléments suivants :*

$$1+\zeta\pi^2, \quad 1+\zeta^2\pi^2, \quad 1+\zeta\pi^2+\zeta\pi^3, \quad 1+\zeta^2\pi^2+\zeta^2\pi^3.$$

Alors, x n'est pas un carré dans K_{nr}.

Démonstration. On raisonne par l'absurde. D'après le lemme 3.4, il existe un élément y dans l'unique extension quadratique non ramifiée N' de $K(\zeta)$ tel que

$$x \equiv y^2 \pmod{4\mathcal{O}_{N'}}.$$

Notons $\mathcal{R}$ un système de représentants du corps résiduel de N' contenant l'ensemble $\{0, 1, \zeta, \zeta^2\}$. Le développement de Hensel de y modulo 2 s'écrit :

$$y \equiv a_0 + a_1\pi \pmod{2\mathcal{O}_{N'}},$$

avec $a_0 \in \mathcal{R} \setminus \{0\}$ et $a_1 \in \mathcal{R}$. Les éléments 2 et π^2 de K étant associés, on en déduit

$$x \equiv y^2 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{N'}}. \tag{3.12}$$

Par unicité du développement de Hensel, on a,

$$a_0^2 = 1 \quad \text{et} \quad a_1^2 = \zeta \text{ ou } \zeta^2.$$

Or, les polynômes X^2-1, $X^2-\zeta$ et $X^2-\zeta^2$ de $\mathcal{O}_{K(\zeta)}[X]$ ont toutes leurs racines dans $\mathcal{O}_{K(\zeta)}$. On en déduit donc :

$$a_0 = 1 \quad \text{et} \quad a_1 = \zeta \text{ ou } \zeta^2.$$

En substituant ces valeurs dans l'équation (3.12), on obtient $x \equiv 1+\zeta\pi^2+\zeta^2\pi^3 \pmod 4$ ou $x \equiv 1 + \zeta^2\pi^2 + \zeta\pi^3 \pmod 4$. D'où une contradiction et le lemme.

3.3.3 Carrés dans l'extension cubique $K(\pi_0)$

Lemme 3.16 *Soit x une unité des entiers de $K(\pi_0)$ congrue modulo 4 à l'un des éléments suivants*

$$1+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10}, \quad 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k,$$

où h et k sont, soit nuls, soit des sommes de puissances > 0 de π_0^3. Alors, x n'est pas un carré dans $K_{nr}(\pi_0)$.

Démonstration. On raisonne par l'absurde. L'extension $K(\pi_0)/\mathbf{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3.5, un élément y de $\mathcal{U}_{K(\pi_0)}$ tel que $x \equiv y^2 \pmod{4\mathcal{O}_{K(\pi_0)}}$. Notons $1+a_1\pi_0+a_2\pi_0^2+a_3\pi_0^3+a_4\pi_0^4+a_5\pi_0^5$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. On a

$$\begin{aligned} x \equiv y^2 \equiv 1 + a_1^2\pi_0^2 + a_2^2\pi_0^4 + a_3^2\pi_0^6 + a_4^2\pi_0^8 + a_5^2\pi_0^{10} + 2a_1\pi_0 + 2a_2\pi_0^2 + 2a_3\pi_0^3 \\ + 2a_4\pi_0^4 + 2a_5\pi_0^5 + 2a_1a_2\pi_0^3 + 2a_1a_3\pi_0^4 + 2a_1a_4\pi_0^5 + 2a_2a_3\pi_0^5 \pmod{4\mathcal{O}_{K(\pi_0)}}. \end{aligned}$$

Si $x \equiv 1 + \pi_0^2 + \pi_0^4 + \pi_0^2h + \pi_0^4k \pmod 4$, alors, par unicité du développement de Hensel, on a $a_1 = a_2 = 1$. Si $a_3 = 1$, le coefficient devant π_0^6 dans le membre de droite de la congruence ci-dessus est non nul, ce qui est absurde. On a donc $a_3 = 0$. Or, $2 \equiv \pi_0^6 \pmod{\pi_0^9}$ car $2 \equiv \pi^2 \pmod{\pi^3}$ů D'où

$$x \equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \equiv 1+\pi_0^2+\pi_0^4+\pi_0^7+(a_4+1)\pi_0^8+\pi_0^9+a_5\pi_0^{10} \pmod 4$$

ce qui est à nouveau absurde car le coefficient devant π_0^9 est nul dans le membre de gauche et non nul dans celui de droite.

Donc nécessairement, $x \not\equiv 1+\pi_0^2+\pi_0^4+\pi_0^2 h+\pi_0^4 k \pmod 4$ et $a_1 = 0$. Autrement dit, le coefficient de π_0^7 dans le développement de x est nul. On en déduit $x \equiv 1+\pi_0^8 \pmod 4$, i.e. $a_1 = a_2 = a_3 = 0$. Comme 2 est associé à π_0^6, il vient alors :

$$x \equiv 1 + a_4\pi_0^8 + a_5^2\pi_0^{10} + 2a_4\pi_0^4 + 2a_5\pi_0^5 \pmod 4 \quad \text{et} \quad a_4 = a_5 = 1.$$

Puis, comme $2 \equiv \pi_0^6 \pmod{\pi_0^9}$, on a $x \equiv 1+\pi_0^8+\pi_0^{11} \pmod 4$. D'où la contradiction et le lemme.

Lemme 3.17 *L'unité $1+\pi_0^8+\pi_0^{11}$ est un carré dans $K_{nr}(\pi_0)$. On a les équivalences suivantes :*

$$1+\pi_0^4+\pi_0^8+\pi_0^{10} \text{ est un carré dans } K_{nr}(\pi_0) \Longleftrightarrow K \in \Omega_1$$

et

$$1+\pi_0^4+\pi_0^8 \text{ est un carré dans } K_{nr}(\pi_0) \Longleftrightarrow K \in \Omega_2.$$

Démonstration. D'après la relation $2 \equiv \pi^2 \pmod{\pi^3}$, on a $2 \equiv \pi_0^6 \pmod{\pi_0^9}$, d'où

$$1+\pi_0^8+\pi_0^{11} \equiv (1+\pi_0^4+\pi_0^5)^2 \pmod 4$$

et le fait que $1+\pi_0^8+\pi_0^{11}$ est un carré dans $K_{nr}(\pi_0)$ (lemme 3.4). Par ailleurs, on a

$$(1+\pi_0^4+\pi_0^8+\pi_0^{10})(1+\pi_0^4+\pi_0^8) \equiv 1+\pi_0^8 \pmod 4$$

et $1+\pi_0^8$ n'est pas un carré dans $K_{nr}(\pi_0)$ d'après le lemme précédent. Autrement dit, si l'un des éléments $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ et $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$, alors l'autre ne l'est pas.

Si $K \in \Omega_1$, d'après la relation (3.9), on a

$$1+\pi_0^4+\pi_0^8+\pi_0^{10} \equiv (1+\pi_0^2+\pi_0^5)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8$ ne l'est pas.

Si $K \in \Omega_2$, d'après la relation (3.10), on a

$$1+\pi_0^4+\pi_0^8 \equiv (1+\pi_0^2)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ ne l'est pas.

D'où les équivalences annoncées.

3.3.4 Carrés dans une extension quadratique ramifiée de K

D'après le lemme 3.12, l'unité $1+\pi^3$ de K n'est pas un carré dans K_{nr}. Notons γ une solution dans $\overline{K}$ de l'équation à coefficients dans $\mathcal{O}_K$

$$X^2 - \frac{2}{\pi}X - \pi = 0. \tag{3.13}$$

Lemme 3.18 *L'élément γ est une uniformisante de $K(\sqrt{1+\pi^3})/K$ et on a*

$$\pi \equiv \gamma^2 + \gamma^3 \pmod 2.$$

Démonstration. D'après l'équation (3.13), on a $v(\gamma) = 1/2$ et $\gamma \in K(\sqrt{1+\pi^3})$. Donc γ est bien une uniformisante de l'extension $K(\sqrt{1+\pi^3})/K$. Par ailleurs, on a $\gamma^2 = (2/\pi)\gamma + \pi$, donc $\gamma^3 = (4/\pi^2)\gamma + 2 + \pi\gamma$. D'où

$$\gamma^2 + \gamma^3 \equiv \frac{2}{\pi}\gamma + \pi + \pi\gamma \equiv \pi \pmod 2,$$

car $4/\pi^2 \equiv 2/\pi + \pi \equiv 0 \pmod 2$. D'où le lemme.

Lemme 3.19 *Soient x un élément de $\mathcal{U}_K$ et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$. On suppose $x \equiv 1+\pi^3 \pmod 4$. Alors, $K_{nr}(\sqrt{x}) = K_{nr}(\sqrt{1+\pi^3})$ et $\sqrt{x} \equiv 1+\gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{x})}}$.*

Démonstration. La première assertion résulte du lemme 3.3. D'après le lemme 3.18, γ est une uniformisante de $K(\sqrt{1+\pi^3})/K$. Notons $a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3$, avec $a_i = 0$ ou 1, le développement de Hensel de $\sqrt{x}$ modulo 2 (il est indépendant du choix de la racine carrée). Alors, d'après le lemme 3.18, on a $\pi^2 \equiv \gamma^4 + \gamma^6 \pmod 4$, $\pi^3 \equiv \gamma^6 + \gamma^7 \pmod 4$ puis, comme 2 est associé à π^2, $2 \equiv \gamma^4 \pmod{\gamma^6}$. Donc

$$\begin{aligned} 1 + \gamma^6 \equiv x &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_0a_1\gamma + 2a_0a_2\gamma^2 \pmod{\gamma^7} \\ &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_0a_1\gamma^5 + (a_3^2 + a_0a_2)\gamma^6 \pmod{\gamma^7}. \end{aligned}$$

Par unicité du développement de Hensel, on en déduit :

$$a_0 = 1, \quad a_1 = a_2 = 0 \quad \text{et} \quad a_3 = 1.$$

D'où le lemme.

Lemme 3.20 *Soit x une unité des entiers de $K(\sqrt{1+\pi^3})$. On suppose que x vérifie l'une des deux conditions suivantes :*

1. *l'unité x est congrue modulo 4 à l'un des quatre éléments*
$$1+\gamma^4+\gamma^6+\gamma^7, \quad 1+\gamma^4, \quad 1+\gamma^6, \quad 1+\gamma^7;$$
2. *on a $x \equiv 1+\gamma^2+\gamma^3 \pmod 2$.*

Alors, x n'est pas un carré dans $K_{nr}(\sqrt{1+\pi^3})$.

Démonstration. On raisonne par l'absurde. L'extension $K(\sqrt{1+\pi^3})/\mathbf{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3.5, une unité y des entiers de $K(\sqrt{1+\pi^3})$ telle que $x \equiv y^2 \pmod 4$. Notons $1+a_1\gamma+a_2\gamma^2+a_3\gamma^3$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. On a alors

$$x \equiv y^2 \equiv 1 + a_1^2\gamma^2 + a_2^2\gamma^4 + 2a_1\gamma + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Par unicité du développement de Hensel, x ne vérifie pas la seconde condition (le coefficient de γ^3 est nul). Il vient alors $a_1 = 0$, puis

$$x \equiv 1 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Or, on a $2 \equiv \gamma^4 \pmod{\gamma^6}$ car $2 \equiv \pi^2 \pmod{\pi^3}$. Donc

$$x \equiv \begin{cases} 1 \pmod 4 & \text{si } (a_2, a_3) = (0,0) \\ 1+\gamma^4+\gamma^6 \pmod 4 & \text{si } (a_2, a_3) = (1,0) \\ 1+\gamma^6+\gamma^7 \pmod 4 & \text{si } (a_2, a_3) = (0,1) \\ 1+\gamma^4+\gamma^7 \pmod 4 & \text{si } (a_2, a_3) = (1,1). \end{cases}$$

D'où la contradiction et le résultat.

3.3.5 Carrés dans $K_{nr}(\sqrt{3})$

D'après le lemme 3.12 et les relations (3.9) et (3.10), 3 est un carré dans K_{nr} si et seulement si K est dans Ω_1. Notons $\sqrt{3}$ une racine carrée de 3 dans $\overline{K}$. Soient x un élément de $\mathcal{U}_K$ et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$.

Lemme 3.21 *Supposons $K \in \Omega_1$ et $x \equiv 3 \pmod 4$. Alors, on a*

$$\sqrt{3} \equiv \sqrt{x} \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}}.$$

Démonstration. Supposons $v(\sqrt{3}-\sqrt{x}) < 2$. Alors, d'après l'égalité, $\sqrt{3}+\sqrt{x} = \sqrt{3}-\sqrt{x}+2\sqrt{x}$, on a $v(\sqrt{3}-\sqrt{x}) = v(\sqrt{3}+\sqrt{x}) < 2$ puis $v(3-x) < 4$ ce qui est absurde. D'où, $v(\sqrt{3}-\sqrt{x}) \geq 2$ ou, autrement dit, $\sqrt{3} \equiv \sqrt{x} \pmod{2\mathcal{O}_{K_{nr}}}$. L'extension $K(\sqrt{x})/K$ est non ramifiée (elle est même éventuellement triviale). En particulier, on peut choisir un système de représentants $\mathcal{R}$ du corps résiduel de $K(\sqrt{x})$ contenu dans $\{0, 1, \zeta, \zeta^2\}$. Notons alors $a_0 + a_1\pi$ le développement de Hensel modulo $2\mathcal{O}_{K_{nr}}$ de $\sqrt{x}$. On a $a_0, a_1 \in \mathcal{R} \subset \{0, 1, \zeta, \zeta^2\}$. Puis, d'après la relation (3.9),

$$3 \equiv 1 + \pi^2 + \pi^3 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Par unicité du développement de Hensel, on en déduit, $a_0 = a_1 = 1$. D'où le lemme.

On suppose désormais $K \in \Omega_2$ de sorte que 3 n'est pas un carré dans K_{nr}.

Lemme 3.22 *Supposons $K \in \Omega_2$. L'unité x est un carré dans $K_{nr}(\sqrt{3})$ si et seulement si $x \equiv 1 \pmod 2$.*

Démonstration. Supposons que x soit un carré dans $K_{nr}(\sqrt{3})$. Il existe alors a et b deux éléments de K_{nr} tels que $x = (a + b\sqrt{3})^2$. Puis, comme $(1, \sqrt{3})$ est une base de l'extension $K_{nr}(\sqrt{3})/K_{nr}$, on a $x = a^2 + 3b^2$ et $ab = 0$. Si $b = 0$, on en déduit que x est un carré dans K_{nr} et si $a = 0$ que $x/3$ est un carré dans K_{nr}. Réciproquement, si x ou $x/3$ est un carré dans K_{nr}, alors x est un carré dans $K_{nr}(\sqrt{3})$. Par ailleurs, d'après le lemme 3.12, x est un carré dans K_{nr} si et seulement si $x \equiv 1 \pmod 4$ ou $x \equiv 1 + \pi^2 + \pi^3 \pmod 4$. De plus, d'après la relation (3.10), on a $3 \equiv 1 + \pi^2 \pmod 4$. Donc, d'après le lemme 3.12, $x/3$ est un carré dans K_{nr} si et seulement si $x \equiv 1+\pi^2 \pmod 4$ ou $x \equiv 1+\pi^3 \pmod 4$. On en déduit le résultat avec l'équivalence précédente.

Notons η une uniformisante de $K(\sqrt{3})$. C'est une extension quadratique de K.

Lemme 3.23 *Supposons $K \in \Omega_2$ et $x \equiv 3 \pmod 4$. Alors, $K_{nr}(\sqrt{x}) = K_{nr}(\sqrt{3})$ et on a*

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \textit{et} \quad \sqrt{x} \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$$

Démonstration. L'égalité résulte du lemme 3.3. L'extension $K(\sqrt{3})/K$ étant totalement ramifiée, π est associé à η^2 et on a

$$\pi \equiv \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \text{ou} \quad \pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

Dans les deux cas, on a, d'après la relation (3.10), $2 \equiv \eta^4 \pmod{\eta^6}$. Notons $a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3$, avec $a_i = 0$ ou 1, le développement de Hensel de $\sqrt{3}$ modulo 2. D'après la relation (3.10), on a alors :

$$3 \equiv 1 + \pi^2 \equiv a_0^2 + a_1^2\eta^2 + a_2^2\eta^4 + a_3^2\eta^6 + 2a_0a_1\eta + 2a_0a_2\eta^2 + 2a_0a_3\eta^3 + 2a_1a_2\eta^3 \pmod 4.$$

Par unicité du développement de Hensel, comme π^2 est associé à η^4, il vient $a_0 = 1$, $a_1 = 0$ et $a_2 = 1$. D'où, comme $2 \equiv \eta^4 \pmod{\eta^6}$,

$$\begin{aligned} 3 &\equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4 \\ &\equiv \begin{cases} 1 + \eta^4 + \eta^6 \pmod 4 & \text{si } a_3 = 0, \\ 1 + \eta^4 + \eta^7 \pmod 4 & \text{si } a_3 = 1. \end{cases} \end{aligned} \tag{3.14}$$

Supposons $\pi \equiv \eta^2 \pmod 2$. Alors, d'après la relation (3.10), on a $2 \equiv \pi^2 \equiv \eta^4 \pmod 4$ et donc, $3 \equiv 1 + \eta^4 \pmod 4$. D'après (3.14), c'est une contradiction. On a donc nécessairement,

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où, $2 \equiv \eta^4 + \eta^6 \pmod{4\mathcal{O}_{K(\sqrt{3})}}$ et, en remplacant dans (3.14),

$$1 + \eta^4 + \eta^6 \equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4.$$

On en déduit $a_3 = 0$. D'où $\sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}}$.

Supposons $v(\sqrt{3} - \sqrt{x}) < 2$. Alors, d'après l'égalité, $\sqrt{3} + \sqrt{x} = \sqrt{3} - \sqrt{x} + 2\sqrt{x}$, on a $v(\sqrt{3} - \sqrt{x}) = v(\sqrt{3} + \sqrt{x}) < 2$ puis $v(3 - x) < 4 = v(4)$ ce qui est absurde. D'où, $v(\sqrt{3} - \sqrt{x}) \geq 2$ ou, autrement dit, $\sqrt{3} \equiv \sqrt{x} \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$. D'où le lemme.

Lemme 3.24 *Supposons $K \in \Omega_2$. L'unité $3 + 2\sqrt{3}$ de l'anneau d'entiers de $K(\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$.*

Démonstration. L'extension $K(\sqrt{3})/\mathbf{Q}_2$ est totalement ramifiée. Supposons que $3 + 2\sqrt{3}$ soit un carré dans $K_{nr}(\sqrt{3})$. Alors, d'après le lemme 3.5, il existe une unité y des entiers de $K(\sqrt{3})$ telle que $3 + 2\sqrt{3} \equiv y^2 \pmod{4\mathcal{O}_{K(\sqrt{3})}}$. Or, d'après le lemme 3.23, on a $3 + 2\sqrt{3} \equiv 1 + 2\eta^2 \equiv 1 + \eta^6 \pmod 4$. Notons $a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. En utilsant la relation $2 \equiv 1 + \eta^4 + \eta^6 \pmod 4$ déduite du lemme 3.23 et de la relation (3.10), on a

$$3 + 2\sqrt{3} \equiv 1 + \eta^6 \equiv a_0^2 + a_1^2\eta^2 + a_2^2\eta^4 + a_0a_1\eta^5 + (a_3^2 + a_0a_2)\eta^6 + (a_0a_1 + a_0a_3 + a_1a_2)\eta^7 \pmod{4\mathcal{O}_{K(\sqrt{3})}}.$$

Par unicité du développement de Hensel, il vient $a_0 = 1$, $a_1 = 0$ et $a_2 = 0$. On a donc

$$1 + \eta^6 \equiv 1 + a_3^2\eta^6 + a_3\eta^7 \pmod{4\mathcal{O}_{K(\sqrt{3})}}.$$

D'où une contradiction car $a_3 = 0$ ou 1. D'où le lemme.

Lemme 3.25 *Soit y une unité des entiers de $K(\sqrt{3})$. On suppose que y est un carré dans $K_{nr}(\sqrt{3})$. Alors,*

$$y \equiv 1 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}} \quad ou \quad y \equiv 1+\eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Démonstration. L'extension $K(\sqrt{3})/\mathbf{Q}_2$ est totalement ramifiée. Comme y est un carré dans $K_{nr}(\sqrt{3})$, il existe d'après le lemme 3.5, une unité z des entiers de $K(\sqrt{3})$ telle que $y \equiv z^2 \pmod 4$. Notons $1+a_1\eta$, avec $a_1 = 0$ ou 1, le développement de Hensel de z modulo η^2. Alors,

$$y \equiv z^2 \equiv 1 + a_1^2\eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où le lemme car $a_1 = 0$ ou 1.

3.3.6 Notations et préliminaires aux démonstrations

On reprend les notations introduites aux sections précédentes en explicitant le choix de la racine cubique $\Delta^{1/3}$ de Δ. D'après le lemme de Hensel appliqué au polynôme $X^3 - \Delta'$ de $\mathcal{O}_K[X]$, Δ' possède une unique racine cubique dans K. On la note δ. On choisit alors de prendre

$$\Delta^{1/3} = \pi_0^{v(\Delta)}\delta$$

de sorte que si $v(\Delta) \equiv 0 \pmod 3$, on a $\Delta^{1/3} \in K$. Notons θ l'unité de K définie par

$$\theta = \varepsilon\frac{\delta}{c_4'}. \tag{3.15}$$

On choisit une racine $B^{1/2}$ de B dans $\overline{K}$ et on pose

$$C = 2(c_4 + 6\Delta^{1/3} + B^{1/2}).$$

Alors,

$$\frac{C}{\pi^{v(c_4)}} = c_4'\left[2\left(1+\frac{B^{1/2}}{c_4}\right) + \theta\pi_0^{12-v(j)}\right] \tag{3.16}$$

est une unité de $K(B^{1/2})$.

Cas où $v(j) < 12$

On a, pour t dans μ_3,

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + 144t^2j^{-2/3} = 1 + t\theta\pi_0^{12-v(j)} + (t\theta\pi_0^{12-v(j)})^2, \tag{3.17}$$

car $12j^{-1/3} = 3(2/\pi^2)^2\pi_0^{12-v(j)}\delta/c_4' = \theta\pi_0^{12-v(j)}$.

Par ailleurs, l'égalité $c_4^3 - c_6^2 = 1728\Delta$ s'écrit

$$\pi^{3v(c_4)}c_4'^3 - \pi^{2v(c_6)}c_6'^2 = 3^3\cdot 2^6\pi^{v(\Delta)}\Delta',$$

puis

$$c_4'^3 - c_6'^2 = \varepsilon^3\pi^{12-v(j)}\Delta', \tag{3.18}$$

car $2v(c_6) = 3v(c_4)$. D'où

$$1 - \frac{c_6'^2}{c_4'^3} = \left(\theta\pi_0^{12-v(j)}\right)^3. \tag{3.19}$$

Lemme 3.26 *Supposons $v(j) \leq 8$. Alors,*

$$c'_4 \equiv c'^3_4 \equiv c'^2_6 \pmod 4.$$

Démonstration. En réduisant l'égalité (3.19) modulo 2, on en déduit avec le lemme 3.11, $c'_4 \equiv 1 \pmod 2$, puis $c'_4 \equiv c'^3_4 \pmod 4$. Les congruences annoncées résultent alors de la même égalité réduite modulo 4, car $v(j) \leq 8$.

Cas où $v(j) = 12$

Pour t dans μ_3, on a

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + 144t^2 j^{-2/3} = 1 + t\theta + (t\theta)^2. \tag{3.20}$$

Le corps K étant totalement ramifié, pour $t = 1$, B/c_4^2 est une unité de $\mathcal{O}_K$.

Par ailleurs, l'égalité $c_4^3 - c_6^2 = 1728\Delta$ s'écrit comme à la relation (3.19),

$$1 - \pi^{2v(c_6)-3v(c_4)} \frac{c'^2_6}{c'^3_4} = \theta^3. \tag{3.21}$$

La somme de deux unités n'en étant pas une, on a $2v(c_6) - 3v(c_4) > 0$.

Cas où $v(j) > 12$

On considère alors la courbe $\widetilde{E}$ d'équation (3.2). Son invariant modulaire $\widetilde{j}$ est de valuation $v(\widetilde{j}) = 24 - v(j) < 12$.

Lemme 3.27 *On a*

$$\widetilde{\Delta}' \equiv c'_4 \pmod 2 \quad \textit{et} \quad j' \cdot \widetilde{j}' \equiv 1 \pmod 4.$$

Démonstration. Cela résulte des lemmes 3.9 et 3.11.

3.3.7 Démonstration du théorème 3.2

L'assertion 1 du théorème 3.2 résulte de l'assertion (i) de [Kra90, th.2]. L'assertion 11 résulte de l'assertion (iv) de [Kra90, th.2] et de la proposition 3.69. On suppose donc désormais que l'on a $1 \leq v(j) \leq 23$. D'où en particulier, $j \neq 0$.

L' assertion 2 lorsque $v(j) \neq 10$ et $v(j) \neq 14$ ainsi que l'assertion 3 résultent directement du théorème 3.1.

Démontrons à présent les autres assertions du théorème 3.2 (la détermination des types de Néron est reportée à la section 3.3.8).

Démonstration de l'assertion 2 lorsque $v(j) = 10$ ou 14

Supposons $v(j) = 10$. On vérifie, avec la relation (3.17) que l'on a

$$\frac{B}{c_4^2} = 1 + \theta\pi_0^2 + (\theta\pi_0^2)^2.$$

Or, $\varepsilon \equiv \pm 1 \pmod 4$ (lemme 3.14), donc, d'après la relation (3.15), $\theta \equiv \pm\delta/c'_4 \pmod 4$. D'après les relations (3.9) et (3.10), on a alors

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^2 + \pi_0^4 + \pi_0^2 h + \pi_0^4 k \pmod 4,$$

où h et k sont, soit nuls, soit des sommes de puissances > 0 de π_0^3. D'après le lemme 3.16, B n'est pas un carré dans M. D'où $|\Phi| = 24$ dans ce cas d'après [Kra90, th.3(ii)].

Supposons $v(j) = 14$. Alors, la courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 10$. Autrement dit, $\widetilde{B}$ n'est pas un carré dans M. D'après la proposition 3.8, il en va de même pour B et donc $|\Phi| = 24$ d'après [Kra90, th.3(ii)].

Démonstration de l'assertion 4

On suppose $v(j) = 4$.

Lemme 3.28 *On a*

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^8 \Delta' \pmod 4.$$

De plus, B est un carré dans M si et seulement si $\Delta' \equiv 1 + \pi \pmod 2$.

Démonstration. D'après les lemmes 3.11 et 3.14, on a

$$\varepsilon \equiv 1 \pmod 2 \quad \text{et} \quad \delta \equiv \Delta' \pmod 2.$$

De plus, d'après les lemmes 3.11 et 3.26, on a $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. D'où, $\theta \equiv \Delta' \pmod 2$, puis $\theta\pi_0^8 \equiv \pi_0^8\Delta' \pmod 4$. La congruence annoncée résulte alors de l'égalité (3.17) appliquée à $t = 1$. On en déduit que B est un carré dans M si et seulement si l'unité $1+\pi_0^8\Delta'$ de l'anneau des entiers de $K(\pi_0)$ l'est (lemme 3.3). Or,

$$1 + \pi_0^8\Delta' \equiv \begin{cases} 1 + \pi_0^8 \pmod 4 & \text{si } \Delta' \equiv 1 \pmod 2 \\ 1 + \pi_0^8 + \pi_0^{11} \pmod 4 & \text{si } \Delta' \equiv 1 + \pi \pmod 2. \end{cases}$$

On conclut à l'équivalence annoncée avec les lemmes 3.16 et 3.17.

Lorsque la condition (C1) n'est pas satisfaite, l'assertion 4 résulte du lemme précédent et de [Kra90, th.3(*ii*)]. Lorsque la condition (C1) est satisfaite, l'assertion 4 se déduit alors du lemme précédent, de l'assertion (*ii*) de [Kra90, th.3] et des propositions 3.45 et 3.46.

Démonstration de l'assertion 10

On suppose $v(j) = 20$. La courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 4$. D'après la proposition 3.8, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après le lemme 3.28, c'est le cas si et seulement si $\widetilde{\Delta}' \equiv 1 + \pi \pmod 2$. D'après le lemme 3.27, c'est équivalent à dire $c_4' \equiv 1 + \pi \pmod 2$.

Lorsque la condition (C1') n'est pas satisfaite, l'assertion 10 résulte de l'équivalence ci-dessus et de l'assertion (*ii*) de [Kra90, th.3]. Lorsque la condition (C1') est satisfaite, l'assertion 10 se déduit alors de l'équivalence ci-dessus, de l'assertion (*ii*) de [Kra90, th.3] et de la proposition 3.64.

Démonstration de l'assertion 5

On suppose $v(j) = 6$.

Lemme 3.29 *On a, pour tout $t \in \mu_3$,*

$$\frac{B_t}{c_4^2} \equiv 1 + t\Delta'\pi^2 \pmod 4.$$

De plus, B_t est un carré dans K_{nr} si seulement si

$$t = 1 \quad et \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration. D'après le lemme 3.14, on a $\varepsilon \equiv 1 \pmod 2$ et d'après le lemme 3.11, $\delta \equiv \Delta' \pmod 2$. Puis d'après le lemme 3.26, $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. On en déduit $\theta \equiv \Delta' \pmod 2$. D'où la congruence annoncée avec la relation (3.17). De plus, B_t est un carré dans K_{nr} si et seulement si l'unité $1 + t\Delta'\pi^2$ de N l'est. Supposons que tel soit le cas. Alors, comme $\Delta' \equiv 1$ ou $1 + \pi \pmod 2$, on a, d'après le lemme 3.15, $t = 1$, puis $\Delta' \equiv 1 + \pi \pmod 2$. Réciproquement, si $t = 1$ et $\Delta' \equiv 1 + \pi \pmod 2$, alors $1 + t\Delta'\pi^2 \equiv (1 + \pi)^2 \pmod 4$ et $B = B_1$ est un carré dans K_{nr}. D'où le lemme.

Supposons $\Delta' \equiv 1 + \pi \pmod 2$. Alors, d'une part, d'après le lemme précédent, $B = B_1$ est un carré dans K_{nr}, donc $|\Phi| = 2$ ou 4, d'après [Kra90, th.3(i)]. D'autre part, B_t pour $t \neq 1$, n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). On en déduit que nécessairement, $|\Phi| = 4$.

Supposons $\Delta' \not\equiv 1 + \pi \pmod 2$. Alors, d'après le lemme précédent, pour tout $t \in \mu_3$, B_t n'est pas un carré dans K_{nr}. Donc d'après la proposition 3.10, on a $|\Phi| = 8$ (on a $c_6 \neq 0$ car $v(j) \neq 12$).

Démonstration de l'assertion 9

Supposons $v(j) = 18$. La courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 6$. D'après la proposition 3.8, si $t \in \mu_3$, B_t est un carré dans K_{nr} si seulement si $\widetilde{B}_{t^2}$ l'est. Or, d'après le lemme 3.29, on a

$$\widetilde{B}_{t^2} \in {K_{nr}}^2 \Longleftrightarrow t = 1 \quad \text{et} \quad \widetilde{\Delta}' \equiv 1 + \pi \pmod 2.$$

D'après le lemme 3.27, on en déduit l'équivalence

$$B_t \in {K_{nr}}^2 \Longleftrightarrow t = 1 \quad \text{et} \quad c_4' \equiv 1 + \pi \pmod 2.$$

L'assertion 9 résulte alors, comme au paragraphe précédent, de l'équivalence ci-dessus et de l'assertion (i) de [Kra90, th.3].

Démonstration de l'assertion 6

Supposons $v(j) = 8$.

Lemme 3.30 *On a*

$$\frac{B}{c_4^2} \equiv 1 + \varepsilon j'\pi_0^4 + \pi_0^8 \pmod 4.$$

De plus, B est un carré dans M si et seulement si $j' \equiv 1 + \pi^2 \pmod{\pi^3}$.

Démonstration. L'élément c'_4/δ est une unité de K, donc d'après le lemme 3.11, on a

$$\left(\frac{c'_4}{\delta}\right)^4 \equiv 1 \pmod 4, \quad \text{d'où } j' = \frac{c'^3_4}{\delta^3} \equiv \frac{\delta}{c'_4} \pmod 4.$$

D'après les lemmes 3.14 et 3.11, on a

$$\varepsilon^2 j'^2 \pi_0^8 \equiv \pi_0^8 \pmod 4.$$

D'où la congruence annoncée d'après (3.17).

Supposons $K \in \Omega_1$. Alors, d'après le lemme 3.14, $\varepsilon \equiv 1 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1+\pi_0^4+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi^2 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi+\pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 3.16 et 3.17 que B est un carré dans M si et seulement si $j' \equiv 1+\pi^2 \pmod{\pi^3}$.

Supposons $K \in \Omega_2$. Alors, d'après le lemme 3.14, $\varepsilon \equiv -1 \equiv 1+\pi^2 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1+\pi_0^4+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi^2 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi+\pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 3.16 et 3.17 que B est un carré dans M si et seulement si $j' \equiv 1+\pi^2 \pmod{\pi^3}$. D'où le lemme.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 6 résulte du lemme ci-dessus et de l'assertion (ii) de [Kra90, th.3]. Lorsque la condition (C2) est satisfaite, l'assertion 6 résulte alors du lemme ci-dessus, de l'assertion (ii) de [Kra90, th.3] et de la proposition 3.53.

Démonstration de l'assertion 8

Supposons $v(j) = 16$. La courbe $\widetilde{E}$ d'équation (3.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 8$. D'après la proposition 3.8, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après l'assertion 6 du théorème 3.2, c'est le cas si et seulement si $\widetilde{j}' \equiv 1+\pi^2 \pmod{\pi^3}$. D'après le lemme 3.27, c'est équivalent à dire $j' \equiv 1+\pi^2 \pmod{\pi^3}$ car on a $j' \equiv 1/\widetilde{j}' \pmod{\pi^3}$.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 8 résulte de l'équivalence ci-dessus et de l'assertion (ii) de [Kra90, th.3]. Lorsque la condition (C2) est satisfaite, l'assertion 8 résulte alors de l'équivalence ci-dessus, de l'assertion (ii) de [Kra90, th.3] et de la proposition 3.58.

Démonstration de l'assertion 7a

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 1$.

Lemme 3.31 *On a, pour t dans μ_3,*

$$\theta \equiv 1+\pi \pmod 2 \quad \textit{et} \quad \frac{B_t}{c_4^2} \equiv 1+t+t^2+t\pi \pmod 2.$$

Démonstration. D'après la relation (3.21), on a $\theta^3 \equiv 1+\pi \pmod 2$. Puis, d'après le lemme 3.11, on a $\theta^2 \equiv 1 \pmod 2$, d'où $\theta \equiv \theta^3 \equiv 1+\pi \pmod 2$. La seconde congruence résulte alors de la première et de la relation (3.20). D'où le lemme.

Supposons $t = 1$. Alors, $B/c_4^2 \equiv 1+\pi \pmod 2$. Donc, d'après le lemme 3.12, B n'est pas un carré dans K_{nr}.

Supposons $t \neq 1$. Alors, $v(B_t) = 1$ est impair. Donc, B_t n'est pas un carré dans K_{nr}.

Autrement dit, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr} . D'après la proposition 3.10, on a $|\Phi| = 8$.

Cela démontre l'assertion 7a du théorème 3.2.

Démonstration de l'assertion 7b

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 2$. En particulier, $v(c_4)$ est pair.

Lemme 3.32 *On a,*

$$\theta \equiv 1 + \pi^2 c_4' \pmod 4 \quad \textit{et} \quad \frac{B}{c_4^2} \equiv 3 + \pi^2 c_4' \pmod 4.$$

Démonstration. D'après la relation (3.21), on a $\theta^3 \equiv 1 \pmod 2$. Donc, d'après le lemme 3.11, on a $\theta \equiv \theta^3 \equiv 1 + \pi^2 c_4' \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (3.20) appliquée à $t = 1$. D'où le lemme.

Lemme 3.33 *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. *on a* $K \in \Omega_1$ *et* $c_4' \equiv 1 + \pi \pmod 2$ *;*
2. *on a* $K \in \Omega_2$ *et* $c_4' \equiv 1 \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}$*, puis*

$$\frac{B^{1/2}}{c_4} \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}} \quad \textit{et} \quad \frac{C}{\pi^{v(c_4)}} \equiv c_4' + \pi^2 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Démonstration. Sous ces hypothèses, on a, d'après les relations (3.9) et (3.10) et le lemme 3.32,

$$\frac{B}{c_4^2} \equiv 1 \pmod 4.$$

D'après le lemme 3.13, il vient $B^{1/2}/c_4 \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$. En particulier,

$$\frac{B^{1/2}}{c_4} + 1 \equiv 0 \pmod{2\mathcal{O}_{K_{nr}}}.$$

Donc, d'après l'égalité (3.16), on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'\theta \pmod{4\mathcal{O}_{K_{nr}}}.$$

Puis, d'après le lemme 3.32, $c_4'\theta \equiv c_4' + \pi^2 \pmod 4$. D'où le résultat annoncé.

On reprend les notations du §3.3.4. En particulier, γ est une uniformisante de $K(\sqrt{1+\pi^3})$.

Lemme 3.34 *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. *on a* $K \in \Omega_1$ *et* $c_4' \equiv 1 \pmod 2$ *;*
2. *on a* $K \in \Omega_2$ *et* $c_4' \equiv 1 + \pi \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3})$ *est une extension quadratique de* K_{nr}*, puis*

$$\frac{B^{1/2}}{c_4} \equiv 1 + \gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}$$

et

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4' + \gamma^4 + \gamma^6 + \gamma^7 \pmod{4\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}.$$

Démonstration. Sous ces hypothèses, on a, d'après les relations (3.9) et (3.10) et le lemme 3.32,

$$\frac{B}{c_4^2} \equiv 1 + \pi^3 \pmod 4.$$

D'après le lemme 3.19, on a donc $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3})$ et $B^{1/2}/c_4 \equiv 1 + \gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}$, d'où la première congruence. Puis, d'après l'égalité (3.16), on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(2\gamma^3 + \theta) \pmod{4\mathcal{O}_{K_{nr}}}.$$

Or, 2 est associé à γ^4, donc $2c_4'\gamma^3 \equiv \gamma^7 \pmod 4$. Et, d'après le lemme 3.18, on a $\pi^2 \equiv \gamma^4 + \gamma^6 \pmod 4$. Donc, d'après le lemme 3.32, on a $c_4'\theta \equiv c_4' + \pi^2 \equiv c_4' + \gamma^4 + \gamma^6 \pmod 4$. D'où le lemme.

On procède comme suit pour la fin de la démonstration de l'assertion 7b.

1. Supposons $K \in \Omega_1$. Si la condition (C1') est satisfaite, on est alors dans un cas d'application du lemme 3.33. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^2$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 3.12, ce n'est jamais le cas car $c_4' + \pi^2 \equiv 1 + \pi \pmod 2$ (condition (C1')). On en déduit que $|\Phi| = 4$ dans ce cas ([Kra90, th.3(i)]).
   Si la condition (C1') n'est pas satisfaite, on est alors dans un cas d'application du lemme 3.34. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c_4' + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$ l'est. Or, d'après le lemme 3.18, on a

$$c_4' + \gamma^4 + \gamma^6 + \gamma^7 \equiv \begin{cases} 1 + \gamma^4 + \gamma^6 + \gamma^7 \pmod 4 & \text{si } c_4' \equiv 1 \pmod 4, \\ 1 + \gamma^7 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^2 \pmod 4, \\ 1 + \gamma^4 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^3 \pmod 4, \\ 1 + \gamma^6 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^2 + \pi^3 \pmod 4. \end{cases}$$

   D'après le lemme 3.20, C n'est donc pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([Kra90, th.3(i)]).
2. Supposons $K \in \Omega_2$. Si la condition (C1') est satisfaite, on est alors dans un cas d'application du lemme 3.34. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c_4' + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$

l'est. Or, $c_4' + \gamma^4 + \gamma^6 + \gamma^7 \equiv c_4' \equiv 1 + \gamma^2 + \gamma^3 \pmod 2$. Donc, d'après le lemme 3.20, C n'est pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([Kra90, th.3(i)]).

Si la condition (C1') n'est pas satisfaite, on est alors dans un cas d'application du lemme 3.33. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^2$ de $\mathcal{O}_K$ l'est. Autrement dit, d'après le lemme 3.12, C est un carré dans K_{nr} si et seulement si $c_4' \equiv 1 + \pi^2 \pmod 4$ ou $c_4' \equiv 1 + \pi^3 \pmod 4$. D'après [Kra90, th.3(i)], on a donc dans ce cas :

$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

Cela achève de démontrer l'assertion 7b du théorème 3.2.

Démonstration de l'assertion 7c

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 3$.

Lemme 3.35 *On a, pour tout t dans μ_3,*

$$\theta \equiv 1 + \pi^3 \pmod 4 \quad \textit{et} \quad \frac{B_t}{c_4^2} \equiv 1 + t + t^2 + t\pi^3 \pmod 4.$$

Démonstration. D'après la relation (3.21), on a $\theta^3 \equiv 1 \pmod 2$ et d'après le lemme 3.11, $\theta^2 \equiv 1 \pmod 2$, d'où, $\theta \equiv 1 \pmod 2$. D'après *loc. cit.* et la relation (3.21) on a alors, $\theta \equiv \theta^3 \equiv 1 + \pi^3 \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (3.20). D'où le lemme.

On déduit du lemme 3.35 que pour $t \neq 1$ dans μ_3, $v(B_t) = 1$ est impair. En particulier, B_t n'est pas un carré dans K_{nr}.

On procède comme suit pour la fin de la démonstration de l'assertion 7c.

1. Supposons $K \in \Omega_1$. Alors, d'après le lemme 3.35 et la relation (3.9), on a

$$\frac{B}{c_4^2} \equiv 3 + \pi^3 \equiv 1 + \pi^2 \pmod 4.$$

   Autrement dit, d'après le lemme 3.12, B n'est pas un carré dans K_{nr}. Par suite, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}. D'après la proposition 3.10, cela implique $|\Phi| = 8$.

2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 3.35 et la relation (3.10), on a

$$\frac{B}{c_4^2} \equiv 3 + \pi^3 \equiv 1 + \pi^2 + \pi^3 \pmod 4.$$

   Autrement dit, d'après le lemme 3.12, B est un carré dans K_{nr}. D'après [Kra90, th.3(i)], on a donc $|\Phi| = 2$ ou 4. Or, pour $t \neq 1$ dans μ_3, B_t n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). Cela implique que l'on a nécessairement $|\Phi| = 4$ dans ce cas.

Cela achève la démonstration de l'assertion 7c du théorème 3.2.

Démonstration de l'assertion 7d

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) \geq 4$.

Lemme 3.36 *On a,*

$$\theta \equiv 1 \pmod 4 \quad \textit{et} \quad \frac{B}{c_4^2} \equiv 3 \pmod 4.$$

Démonstration. D'après la relation (3.21), on a $\theta^3 \equiv 1 \pmod 2$ et d'après le lemme 3.11, $\theta^2 \equiv 1 \pmod 2$, d'où, $\theta \equiv 1 \pmod 2$. D'après *loc. cit.* et la relation (3.21) on a alors, $\theta \equiv \theta^3 \equiv 1 \pmod 4$. La seconde congruence résulte alors de l'égalité (3.20). D'où le lemme.

Lemme 3.37 *Supposons $K \in \Omega_1$. Alors, $K_{nr}(B^{1/2}) = K_{nr}$ et on a*

$$\frac{B^{1/2}}{c_4} \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}} \quad \textit{et} \quad \frac{C}{\pi^{v(c_4)}} \equiv c_4' + \pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Démonstration. D'après le lemme 3.36, on a $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$. Or, 3 est un carré dans K_{nr} car K est dans Ω_1. D'où l'égalité annoncée. La première congruence résulte du lemme 3.21 et de la congruence $B/c_4^2 \equiv 3 \pmod 4$ du lemme 3.36. D'après l'égalité (3.16), le lemme 3.36 et la première congruence ci-dessus, on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(2\pi + 1) \pmod{4\mathcal{O}_{K_{nr}}}.$$

D'où le résultat car $2c_4'\pi \equiv \pi^3 \pmod 4$.

On reprend les notations du §3.3.5. En particulier, η désigne, lorsque $K \in \Omega_2$, une uniformisante de $K(\sqrt{3})$.

Lemme 3.38 *Supposons $K \in \Omega_2$. Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ et on a*

$$\frac{B^{1/2}}{c_4} \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$$

et

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(3 + 2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Démonstration. L'égalité et la première congruence résultent des lemmes 3.36 et 3.23. La seconde résulte de la première congruence, du lemme 3.36 et de l'égalité (3.16).

On procède comme suit pour la fin de la démonstration de l'assertion 7d.

1. Supposons $K \in \Omega_1$. Si $v(c_4) = v(C)$ est impair, alors C n'est pas un carré dans $K_{nr}(B^{1/2}) = K_{nr}$. Donc $|\Phi| = 4$ d'après [Kra90, th.3(i)]. Si $v(c_4)$ est pair. Alors, d'après le lemme 3.37, B est un carré dans K_{nr}. De plus, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^3$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 3.12, c'est le cas si et seulement si la condition (C3) est satisfaite. D'où le résultat d'après [Kra90, th.3(i)].

2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 3.38, B n'est pas un carré dans K_{nr}. Si $v(c_4)$ est impair, on a

$$\frac{C}{\pi^{v(c_4)-1}\eta^2} \equiv c_4'\beta(3+2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}},$$

où β est une unité des entiers de $K(\sqrt{3})$ telle que $\pi = \eta^2\beta$. On en déduit que C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'\beta(3+2\sqrt{3})$ de $K(\sqrt{3})$ est un carré dans $K_{nr}(\sqrt{3})$. Or, d'après le lemme 3.23, on a $\beta \equiv 1+\eta \pmod{\eta^2}$. D'où $c_4'\beta(3+2\sqrt{3}) \equiv 1+\eta \pmod{\eta^2}$. On en déduit, avec le lemme 3.25 que C n'est pas un carré dans $K_{nr}(\sqrt{3})$. D'où $|\Phi| = 8$ dans ce cas d'après [Kra90, th.3(i)].
Supposons $v(c_4)$ pair. Alors, C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'(3+2\sqrt{3})$ de $K(\sqrt{3})$ l'est. Si c_4' est un carré dans $K_{nr}(\sqrt{3})$, alors C n'est pas un carré dans $K_{nr}(\sqrt{3})$, car d'après le lemme 3.24, $3+2\sqrt{3}$ ne l'est pas. Si c_4' n'est pas un carré dans $K_{nr}(\sqrt{3})$, alors d'après le lemme 3.22, on a $c_4' \equiv 1+\pi \pmod 2$. D'après le lemme 3.23, on a alors

$$c_4'(3+2\sqrt{3}) \equiv 1+\pi \equiv 1+\eta^2+\eta^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Donc, d'après le lemme 3.25, $c_4'(3+2\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$ et il en va de même pour C d'après l'équivalence ci-dessus. D'où $|\Phi| = 8$ dans ce cas d'après [Kra90, th.3(i)].

Cela achève la démonstration de l'assertion 7d du théorème 3.2.

3.3.8 Calculs des types de Néron

D'après [Tat75], la courbe E admet un modèle de Weierstrass de la forme

$$Y^2 = X^3 - \frac{c_4}{48}X - \frac{c_6}{864}. \qquad (W_0)$$

Ce modèle est entier si et seulement si on a $v(c_4) \geq 8$ et $v(c_6) \geq 10$. Dans toute cette section, on note Δ_m le discriminant minimal de E.

Cas où $v(j) = 4$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 4$ et la condition (C1), i.e. $\Delta' \equiv 1+\pi \pmod 2$. D'après la formule (3.18), on a

$$c_4'^3 - c_6'^2 = \varepsilon^3\pi^8\Delta', \qquad (3.22)$$

où l'on a posé $\varepsilon = 3\left(\frac{2}{\pi^2}\right)^2$.

Lemme 3.39 *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV^*. Alors, on a $v(\Delta_m) = 8$.*

Démonstration. D'après [Kra90, th.2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. C'est en contradiction avec la condition $v(j) = 4$. Par ailleurs, si E est de type IV^*, on a alors $v(\Delta_m) = 8$. D'où le lemme.

Lemme 3.40 *Supposons* $v(\Delta) \equiv 8 \pmod{12}$. *Alors,* $v(\Delta_m) = 8$ *si et seulement si* $c_6' \equiv 1 \pmod 2$.

Démonstration. Supposons $v(\Delta) \equiv 8 \pmod{12}$. D'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 12, 20).$$

La courbe E correspond alors à un cas 7 de Tate ou à un cas non minimal. Le modèle (W_0) de E est entier et, avec les notations de [Tat75], on a

$$b_2 = 0; \quad b_4 = -2\frac{c_4}{48} = -6\frac{c_4'}{\varepsilon^2}; \quad b_6 = -4\frac{c_6}{864} = -2^3\frac{c_6'}{\varepsilon^3};$$

$$b_8 = -\left(\frac{c_4}{48}\right)^2 = -3^2\frac{c_4'^2}{\varepsilon^4}.$$

Examinons à présent à quelle condition le système suivant de congruences admet une solution (r, s) dans $\mathcal{O}_K$:

$$\begin{cases} b_8 + 3r^2 b_4 + 3r^4 \equiv 0 \pmod{4\pi} \\ r \equiv s^2 \pmod 2. \end{cases}$$

Comme $v(b_8) = 0$, si (r, s) est une solution, on a nécessairement $r \in \mathcal{U}_K$, donc s est également une unité et, d'après la seconde congruence, $r \equiv 1 \pmod 2$ (et on peut choisir $s = 1$). On a alors, $r^2 \equiv r^4 \equiv 1 \pmod{4\pi}$ et de même, $\varepsilon^2 \equiv \varepsilon^4 \equiv 1 \pmod{4\pi}$. Donc

$$-9c_4'^2 - 18c_4' + 3 \equiv 0 \pmod{4\pi}.$$

Autrement dit, le système précédent admet une solution si et seulement si $c_4'^2 + 2c_4' \equiv 3 \pmod{4\pi}$. Or, d'après la relation (3.22) et le lemme 3.11, on a $c_4' \equiv 1 \pmod 2$, puis $c_4'^2 \equiv 1 \pmod{4\pi}$ et $c_4' \equiv c_6'^2 \pmod{4\pi}$. Donc, on a $3 \equiv c_4'^2 + 2c_4' \equiv 1 + 2c_6'^2 \pmod{4\pi}$. Mais, par ailleurs, on a

$$1 + 2c_6'^2 \equiv \begin{cases} 3 \pmod{4\pi} & \text{si } c_6' \equiv 1 \pmod 2 \\ 3 + \pi^4 \pmod{4\pi} & \text{si } c_6' \equiv 1 + \pi \pmod 2. \end{cases}$$

On en déduit qu'il existe une solution (r, s) au système de congruences ci-dessus si et seulement si $c_6' \equiv 1 \pmod 2$. On conclut alors au lemme avec [Pap93, prop.4].

Lemme 3.41 *Supposons* $c_6' \equiv 1 \pmod 2$. *Alors, on a*

$$c_4' \equiv (1 + \pi^4)(1 - c_6'^2) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Démonstration. On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où, $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 3.14). En réduisant l'égalité (3.22) modulo 2, on obtient $c_4' \equiv 1 \pmod 2$. Puis, d'après le lemme 3.11, on a $c_4' \equiv c_4'^3 \pmod{4\pi}$ et, comme $c_6' \equiv 1 \pmod 2$, $c_6'^2 \equiv 1 \pmod{4\pi}$. Comme d'après la relation (3.22), on a $c_4'^3 \equiv c_6'^2 \pmod{4\pi}$, il vient $c_4' \equiv 1 \pmod{4\pi}$. On en déduit $c_4'^2 \equiv 1 \pmod{\pi^7}$, puis $c_4'^3 \equiv c_4' \pmod{\pi^7}$. D'où $c_4' \equiv c_6'^2 \pmod{\pi^7}$ avec la relation (3.22) réduite modulo π^7. Posons donc $c_4' = c_6'^2 + \pi^7 a$, avec $a \in \mathcal{O}_K$. On a

$$c_4'^3 \equiv c_6'^6 + 3\pi^7 c_6'^4 a \pmod{\pi^{10}}.$$

Or, $c_6'^4 \equiv 1 \pmod{\pi^3}$ et $3 \equiv 1+\pi^2 \pmod{\pi^3}$, donc $c_4'^3 \equiv c_6'^6 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}$, puis

$$c_4'^3 - c_6'^2 \equiv c_6'^6 - c_6'^2 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}.$$

Mais, comme $c_6'^2 \equiv 1 \pmod{\pi^5}$ car $c_6' \equiv 1 \pmod 2$, on a $c_6'^2 + 1 \equiv 2 \pmod{\pi^5}$ et

$$c_6'^6 - c_6'^2 = c_6'^2(c_6'^2+1)(c_6'^2-1) \equiv 2(c_6'^2-1) \equiv 2(c_4' - \pi^7 a - 1) \pmod{\pi^{10}}.$$

Autrement dit, on a $c_4'^3 - c_6'^2 \equiv 2c_4' - 2 - \pi^7 a + \pi^9 a \pmod{\pi^{10}}$ et $c_4'^3 - c_6'^2 \equiv c_4' + c_6'^2 - 2 + \pi^9 a \pmod{\pi^{10}}$. Par ailleurs, d'après l'hypothèse (C1), on a $c_4'^3 - c_6'^2 \equiv \pi^8 + \pi^9 \pmod{\pi^{10}}$. On en déduit donc

$$c_4' \equiv -c_6'^2 + 2 + \pi^8 + \pi^9(a+1) \pmod{\pi^{10}}.$$

Or, on a $\pi^9(a+1) = \pi^2(c_4' - c_6'^2 + \pi^7)$. Donc $(1-\pi^2)c_4' \equiv -(1+\pi^2)c_6'^2 + 2 + \pi^8 + \pi^9 \pmod{\pi^{10}}$. D'où

$$c_4' \equiv \frac{1+\pi^2}{1-\pi^2}(1-c_6'^2) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Enfin, on a $(1+\pi^2)/(1-\pi^2) \equiv 1+\pi^4 \pmod{\pi^5}$ et donc le résultat car $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$. Cela démontre le lemme.

Posons

$$a_2 = \frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right); \quad a_4 = \frac{1}{\pi^4}\left(\frac{3}{\varepsilon^2}\left(c_6'^2 - c_4'\right) - 4\right);$$

$$a_6 = \frac{1}{\pi^6}\left(\frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3c_4' - 2\right) - 4\right).$$

Proposition 3.42 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. *Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E *pour lequel on a*

$$a_4 \equiv \frac{1}{\pi^2}\left(c_6'^2 - 1\right) + \varepsilon \pmod 4, \quad a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^2 + \pi^3 \pmod 4$$

et

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4, \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Démonstration. Le changement de variables

$$X = x + \frac{1}{\pi^2}\frac{c_6'}{\varepsilon}; \qquad Y = y + \frac{x}{\pi} + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Les éléments $2/\pi$ et $4/\pi^3$ sont entiers. D'après le lemme 3.40, on a $c_6' \equiv 1 \pmod 2$. Donc, d'après le lemme 3.14, le coefficient a_2 est entier. Vérifions que

les coefficients a_4 et a_6 le sont aussi et qu'ils satisfont aux congruences annoncées. D'après le lemme 3.41, on a

$$\begin{aligned}\pi^4 a_4 &\equiv \frac{3}{\varepsilon^2}\left(c_6'^2 - (1+\pi^4)(1-c_6'^2) - 1\right) - 4 \pmod{\pi^8}\\ &\equiv \frac{3}{\varepsilon^2}(2+\pi^4)(c_6'^2-1) - 4 \pmod{\pi^8}.\end{aligned}$$

Or, $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$, donc $v(a_4) = 0$ et a_4 est une unité de $\mathcal{O}_K$. Puis, on a $\pi^4 a_4 \equiv 2(c_6'^2-1) - 4 \pmod{\pi^8}$ et

$$a_4 \equiv \left(\frac{2}{\pi^2}\right)\frac{1}{\pi^2}(c_6'^2-1) - \left(\frac{2}{\pi^2}\right)^2 \pmod 4.$$

On en déduit la congruence annoncée pour a_4 car $v(c_6'^2-1) \geq 5$ et $2/\pi^2$ est une unité.

Examinons à présent le coefficient a_6. On a, d'après le lemme 3.41,

$$\begin{aligned}\pi^6 a_6 &= \frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3c_4' - 2\right) - 4\\ &\equiv \frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3(1+\pi^4)(1-c_6'^2) - 5\right) + \pi^8 + \pi^9 - 4 \pmod{\pi^{10}}\\ &\equiv \frac{c_6'}{\varepsilon^3}\left((4+3\pi^4)(c_6'^2-1) - 4\right) + \pi^8 + \pi^9 - 4 \pmod{\pi^{10}}.\end{aligned}$$

Or, $4 + 3\pi^4 \equiv 0 \pmod{\pi^5}$ et $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$, donc $\pi^6 a_6 \equiv -4c_6'/\varepsilon^3 - 4 + \pi^8 + \pi^9 \pmod{\pi^{10}}$. Puis, comme $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, on a

$$\pi^6 a_6 \equiv -4\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

D'où $v(a_6) \geq 0$ car $c_6'/\varepsilon + 1 \equiv 0 \pmod 2$ et on a

$$a_6 \equiv -\left(\frac{2}{\pi^2}\right)^2 \frac{1}{\pi^2}\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^2 + \pi^3 \pmod 4.$$

D'où la congruence annoncée pour a_6 par définition de ε.

On en déduit que l'on a

$$3a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6' + 3\right) + \pi^2 + \pi^3 \pmod 4.$$

Or, $3 \equiv -5 \equiv -1 - 4 \pmod{\pi^6}$, donc

$$3a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right) - \frac{4}{\pi^2}\varepsilon + \pi^2 + \pi^3 \pmod 4.$$

Or, $4 \equiv \pi^4 \pmod{\pi^6}$, donc, par définition du coefficient a_2, on a $3a_6 \equiv \varepsilon a_2 + \pi^3 \pmod 4$. C'est la congruence voulue.

Enfin, on a, par définition du coefficient a_2,

$$\begin{aligned}\pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) &= \frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right)\left(\frac{3}{\varepsilon}c_6' + 1\right) \equiv \frac{1}{\pi^2}\left(\frac{9}{\varepsilon^2}c_6'^2 - 1\right) \pmod 4\\ &\equiv \frac{1}{\pi^2}(c_6'^2 - 1) \pmod 4 \quad \text{car } 9/\varepsilon^2 \equiv 1 \pmod{\pi^6}\\ &\equiv a_4 - \varepsilon \pmod 4\end{aligned}$$

d'après la première congruence. Cela achève la démonstration de la proposition 3.42.

Posons

$$r = \frac{2}{\pi^2} + \pi \quad \text{et} \quad t = \pi.$$

Notons b_2, b_4, b_6 et b_8 les invariants standard associés au modèle (W) de E.

Lemme 3.43 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. *Alors, on a*

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{\pi^5}.$$

De plus, la courbe E correspond à un cas ≥ 7 de Tate si et seulement si on a $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$.

Démonstration. On considère le modèle (W) de E de la proposition 3.42. On a

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = \frac{2^3}{\pi^4} + 2a_4; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6;$$

et

$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2.$$

On en déduit que l'on a les congruences suivantes :

$$b_2 \equiv -\varepsilon\pi^2 + 4a_2 \pmod{4\pi}, \qquad b_4 \equiv 2(a_4 - \varepsilon) \equiv 0 \pmod{4\pi},$$

$$b_6 \equiv \pi^2 + 4a_2 \pmod{4\pi}, \qquad b_8 \equiv \pi^2(a_2 - \varepsilon a_6) + 1 + 4a_2 \equiv 1 \pmod{4\pi}$$

car $a_2 - \varepsilon a_6 \equiv 2a_2 \pmod{\pi^3}$.

L'entier r de $\mathcal{O}_K$ est une unité de $\mathcal{O}_K$ et on a

$$\begin{aligned} b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 &\equiv 1 + 3r\pi^2 + 4a_2 - \varepsilon r^3\pi^2 + 4a_2 + 3 \pmod{4\pi} \\ &\equiv 4 + \pi^2(3 - \varepsilon r^2) \pmod{4\pi} \\ &\equiv 4 + \pi^2\left(\left(\frac{2}{\pi^2}\right)^2 - r^2\right) \pmod{4\pi}. \end{aligned}$$

Or, $r^2 \equiv (2/\pi^2)^2 + \pi^2 \pmod{\pi^3}$. Donc $4 + \pi^2((2/\pi^2)^2 - r^2) \equiv 0 \pmod{4\pi}$. Autrement dit, $r = 2/\pi^2 + \pi$ vérifie la condition (a) de [Pap93, prop. 3]. On a alors, d'après les congruences de la proposition 3.42,

$$\begin{aligned} a_6 + ra_4 + r^2a_2 + r^3 &= a_6 + \left(\frac{2}{\pi^2} + \pi\right)a_4 + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \\ &\equiv \pi^3 - \varepsilon a_2 + \left(\frac{2}{\pi^2} + \pi\right)\left(\varepsilon + \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right)\right) \\ &\quad + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \pmod 4 \qquad (3.23) \\ &\equiv \pi^3 - \varepsilon a_2 + \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2a_2\left(a_2 + \frac{2}{\pi^2}\right) - \varepsilon a_2 + \frac{4}{\pi}a_2 + \pi^2 a_2 \\ &\quad - \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2 + \pi^3 \pmod 4 \\ &\equiv \pi^3(a_2+1) + 2a_2(a_2+1) + 2 \equiv (a_2+1)(\pi^3+2a_2) + 2 \pmod 4. \end{aligned}$$

Par ailleurs, on a $v((a_2+1)(\pi^3+2a_2)) \geq 3$, donc en particulier,

$$a_6 + ra_4 + r^2a_2 + r^3 \equiv 2 \equiv \pi^2 \pmod{\pi^3}.$$

On a alors, avec $t = \pi$,

$$\begin{aligned} t\left(\frac{4}{\pi^3}\right) + t^2 + rt\left(\frac{2}{\pi}\right) &\equiv \pi^2\left(\frac{2}{\pi^2}\right)^2 + \pi^2 + 2\left(\frac{2}{\pi^2} + \pi\right) \pmod 4 \\ &\equiv \pi^2 + \pi^2 + \pi^2 + \pi^3 \pmod 4 \\ &\equiv \pi^2 + \pi^3 \pmod 4. \end{aligned} \tag{3.24}$$

Donc, en particulier, $t(4/\pi^3) + t^2 + rt(2/\pi) \equiv \pi^2 \pmod{\pi^3}$. On déduit alors de [Pap93, prop. 3] appliqué à r et t et des congruences (3.23) et (3.24) que l'on est dans un cas ≥ 7 de Tate si et seulement si $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. D'où le lemme.

Lemme 3.44 *Supposons $c_6' \equiv 1 \pmod 2$. Alors, $v((a_2+1)(\pi^3+2a_2)) \geq 3$. De plus, on a $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ si et seulement si $a_2 \equiv 0$ ou $1+\pi \pmod 2$.*

Démonstration. D'après l'hypothèse faite, le coefficient a_2 est entier et l'on a $v((a_2+1)(\pi^3+2a_2)) \geq 3$. De plus, $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ si et seulement si $v((a_2+1)(\pi^3+2a_2)) = 3$. Or, $v((a_2+1)(\pi^3+2a_2)) = 3$ si et seulement si $v(a_2) \geq 2$ ou $v(a_2+1) = 1$. D'où le résultat.

Proposition 3.45 *Supposons $K \in \Omega_1$. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 8 \pmod{12}$;*
2. *on a $c_6' \equiv 1+\pi^2 \pmod 4$ ou $c_6' \equiv 1+\pi^3 \pmod 4$.*

Démonstration. Supposons $|\Phi| = 3$. D'après [Kra90, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 3.39, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut de plus supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. Puis, d'après le lemme 3.40, on a $c_6' \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 3.43, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_1, il vient $(a_2+1)(\pi^3+2a_2) \equiv 0 \pmod 4$. Autrement dit, d'après le lemme 3.44, on a $a_2 \equiv 1$ ou $\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_1, on a, d'après le lemme 3.14,

$$\begin{aligned} \pi^2 a_2 \equiv -c_6' - 1 \pmod 4, \text{ d'où } c_6' &\equiv \pi^2 a_2 - 1 \\ &\equiv \pi^2 a_2 + 1 + \pi^2 + \pi^3 \pmod 4. \end{aligned}$$

On en déduit que l'on a $c_6' \equiv 1+\pi^2 \pmod 4$ ou $c_6' \equiv 1+\pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 3.40, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. D'après l'appendice 3.5, E correspond alors à un cas 6, 7 ou 8 (type IV^*) de Tate. Par ailleurs, comme K est dans Ω_1, on a $a_2 \equiv (3c_6'-1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 1$ ou $\pi \pmod 2$. Donc, d'après le lemme 3.44, on a $(a_2+1)(\pi^3+2a_2) \equiv$

$0 \pmod 4$, puis, comme K est dans Ω_1, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Autrement dit, d'après le lemme 3.43, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est alors dans un cas 8 de Tate. Toujours d'après le lemme 3.43, comme la condition (a) de [Pap93, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 1$ ou $\pi \pmod 2$ et $r \equiv 1 \pmod 2$. En effet, on a ou bien $a_2 + 1 \equiv 0 \pmod 2$ et on choisit $s = 0$, ou bien $a_2 + 1 \equiv 1 + \pi \pmod 2$ et on choisit $s = 1$. La condition (b) de [Pap93, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [Kra90, th.2(i)]. Cela démontre la proposition.

Proposition 3.46 *Supposons $K \in \Omega_2$. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. $v(\Delta) \equiv 8 \pmod{12}$;
2. $c_6' \equiv 1 \pmod 4$ *ou* $c_6' \equiv 1 + \pi^2 + \pi^3 \pmod 4$.

Démonstration. Supposons $|\Phi| = 3$. D'après [Kra90, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 3.39, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut de plus supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Puis, d'après le lemme 3.40, on a $c_6' \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 3.43, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_2, il vient $(a_2 + 1)(\pi^3 + 2a_2) \equiv \pi^3 \pmod 4$. Autrement dit, d'après le lemme 3.44, on a $a_2 \equiv 0$ ou $1+\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_2, on a, d'après le lemme 3.14,

$$\pi^2 a_2 \equiv c_6' - 1 \pmod 4, \text{ d'où } c_6' \equiv \pi^2 a_2 + 1 \pmod 4.$$

On en déduit que l'on a $c_6' \equiv 1 \pmod 4$ ou $c_6' \equiv 1 + \pi^2 + \pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 3.40, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. D'après l'appendice 3.5, E correspond à un cas 6, 7 ou 8 (type IV^*) de Tate. Par ailleurs, comme K est dans Ω_2, on a $a_2 \equiv (c_6' - 1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 0$ ou $1+\pi \pmod 2$. Donc, d'après le lemme 3.44, on a $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$, puis, comme K est dans Ω_2, $(a_2 + 1)(\pi^3 + 2a_2) + 2 \equiv \pi^2 + \pi^3 \pmod 4$. Autrement dit, d'après le lemme 3.43, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est alors dans un cas 8 de Tate. Toujours d'après le lemme 3.43, comme la condition (a) de [Pap93, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 0$ ou $1 + \pi \pmod 2$ et $r \equiv 1 + \pi \pmod 2$. En effet, on a ou bien $a_2 + 1 + \pi \equiv 1 + \pi \pmod 2$ et on choisit $s = 1$, ou bien $a_2 + 1 + \pi \equiv 0 \pmod 2$ et on choisit $s = 0$. La condition (b) de [Pap93, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [Kra90, th.2(i)]. Cela démontre la proposition.

Cas où $v(j) = 8$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 8$ et la condition (C2), i.e. $j' \equiv 1 + \pi^2 \pmod{2\pi}$. D'après la formule (3.18), on a

$$c_4'^3 - c_6'^2 = \varepsilon^3 \pi^4 \Delta'. \tag{3.25}$$

Lemme 3.47 *La courbe E n'est pas de type IV^*. Supposons qu'elle soit de type IV. Alors, on a $v(\Delta_m) = 4$.*

Démonstration. D'après [Kra90, th.2(i)], si E est de type IV^*, on a $v(\Delta_m) = 8$. C'est en contradiction avec la condition $v(j) = 8$. Par ailleurs, si E est de type IV, on a $v(\Delta_m) = 4$. D'où le lemme.

Lemme 3.48 *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, $v(\Delta_m) = 4$ si et seulement si $c_6' \equiv 1 \pmod 2$.*

Démonstration. Supposons $v(\Delta) \equiv 4 \pmod{12}$. D'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 12, 16).$$

Le modèle (W_0) de E est alors entier et la courbe E correspond à un cas 7 de Tate ou à un cas non minimal. Exactement comme dans la démonstration du lemme 3.39, on montre qu'il n'est pas minimal si et seulement si on a $c_6' \equiv 1 \pmod 2$. D'où le lemme.

Lemme 3.49 *Supposons $c_6' \equiv 1 \pmod 2$. On a $c_4' \equiv c_6'^2 + \varepsilon\pi^4 \pmod{\pi^7}$.*

Démonstration. On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où, $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 3.14). En réduisant l'égalité (3.25) modulo 2, on obtient $c_4' \equiv 1 \pmod 2$. Puis, d'après le lemme 3.11, on a $c_4' \equiv c_4'^3 \pmod{4\pi}$ et $c_6'^2 \equiv 1 \pmod{4\pi}$ car $c_6' \equiv 1 \pmod 2$. Comme d'après la relation (3.25), on a $c_4'^3 \equiv c_6'^2 + \pi^4 \pmod{4\pi}$, il vient

$$c_4' \equiv 1 + \pi^4 \pmod{4\pi}. \tag{3.26}$$

On en déduit $c_4'^2 \equiv 1 + 2\pi^4 \equiv 1 + \pi^6 \pmod{4\pi^3}$, puis

$$c_4'^3 \equiv c_4' + \pi^6 \pmod{4\pi^3}. \tag{3.27}$$

Par ailleurs, d'après la relation (3.26), on a, en particulier, $c_4' \equiv 1 \pmod{2\pi}$, donc l'hypothèse $j' \equiv 1 + \pi^2 \pmod{2\pi}$ implique

$$\Delta' \equiv 1 + \pi^2 \pmod{2\pi}. \tag{3.28}$$

Autrement dit, on a, d'après l'égalité (3.25) et la congruence (3.27),

$$c_4' \equiv c_6'^2 + \varepsilon\pi^4 \pmod{\pi^7},$$

car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$ donc, en particulier, $\varepsilon^2 \equiv 1 \pmod{2\pi}$. D'où le résultat.

Posons

$$a_2 = \frac{1}{\pi^2}\left(3\varepsilon c_6' - 1\right); \quad a_4 = \frac{1}{\pi^4}\frac{3}{\varepsilon^2}\left(\varepsilon^4 c_6'^2 - c_4'\right);.$$

$$a_6 = \frac{1}{\pi^6}\frac{c_6'}{\varepsilon^3}\left(\varepsilon^6 c_6'^2 - 3c_4'\varepsilon^2 - 2\right).$$

Proposition 3.50 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6, \qquad (W)$$

définit un modèle de Weierstrass entier de E *pour lequel on a* $a_4 \equiv 1 \pmod 2$ *et* $a_6 \equiv 1 \pmod \pi$.

Démonstration. Le changement de variables

$$X = x + \frac{\varepsilon c_6'}{\pi^2}; \qquad Y = y + \frac{x}{\pi}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $2/\pi$ est entier. D'après le lemme 3.48, on a $c_6' \equiv 1 \pmod 2$. De plus, d'après le lemme 3.14, le coefficient a_2 est entier. Vérifions que les coefficients a_4 et a_6 sont entiers et satisfont aux congruences annoncées.

On a

$$\pi^4 a_4 = \frac{3}{\varepsilon^2}(\varepsilon^4 c_6'^2 - c_4') \equiv \frac{3}{\varepsilon^2}(c_6'^2 - c_4') \equiv 3\frac{\pi^4}{\varepsilon^2} \equiv \pi^4 \pmod{\pi^6},$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^6}$ et, d'après le lemme 3.49, $c_4' \equiv c_6'^2 + \pi^4 \pmod{\pi^6}$. D'où le fait que $a_4 \equiv 1 \pmod 2$.

Examinons à présent le coefficient a_6. On a, d'après le lemme 3.49,

$$\begin{aligned}\frac{\varepsilon^3}{c_6'}\pi^6 a_6 &\equiv \varepsilon^2 c_6'^2 - 3c_4'\varepsilon^2 - 2\varepsilon^2 \pmod{4\pi^3} \\ &\equiv \varepsilon^2(c_6'^2 - 3c_4' - 2) \equiv \varepsilon^2(-2c_4' - 2 - \varepsilon\pi^4) \pmod{4\pi^3},\end{aligned}$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^7}$. Or, $-\varepsilon\pi^4 = -12$ et, d'après le lemme 3.49 et la congruence $c_6' \equiv 1 \pmod 2$, on a $c_4' + 1 \equiv 2 + \pi^4 \pmod{4\pi}$. Donc

$$\frac{\varepsilon^3}{c_6'}\pi^6 a_6 \equiv -2\pi^4 \equiv \pi^6 \pmod{4\pi^3}.$$

Comme ε^3/c_6' est une unité de $\mathcal{O}_K$, il en résulte $a_6 \equiv 1 \pmod \pi$ et la proposition.

Lemme 3.51 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors,* E *ne correspond pas à un cas* 4 *de Tate.*

Démonstration. D'après l'appendice 3.5, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 3.50. Supposons qu'il corresponde à un cas ≥ 4 de Tate. D'après la congruence $a_4 \equiv 1 \pmod 2$, $r = 1$ satisfait à la première relation de divisibilité de [Pap93, prop. 2]. On a par ailleurs, avec les notations de [Tat75],

$$b_2 \equiv \pi^2 \pmod{2\pi}; \quad b_4 \equiv \pi^2 \pmod{2\pi}; \quad b_6 \equiv 0 \pmod{2\pi};$$

$$b_8 \equiv \pi^2 a_6 - 1 \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv \pi^2 a_6 + 2 \equiv \pi^2(a_6 + 1) \pmod{2\pi}$. D'où le résultat d'après [Pap93, prop. 2] et la congruence $a_6 \equiv 1 \pmod \pi$.

Lemme 3.52 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors,* a_2 *et* a_6 *sont entiers et on a*

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c_6' + 1) \pmod 2, \quad c_6' \equiv \pi^2 a_2 - \varepsilon \pmod 4.$$

et

$$a_6 \equiv \frac{1}{\pi^6}(c_6'^2 - 3c_4' - 2) \pmod 2, \quad c_4' \equiv -c_6'^2 + 6 + \pi^6 a_6 \pmod{\pi^8}.$$

Démonstration. Les éléments a_2 et a_6 sont entiers d'après la proposition 3.50. On a, $3\varepsilon \equiv -\varepsilon \pmod 4$, d'où les deux premières congruences. De plus, on a $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ et $2 \equiv 2\varepsilon^2 \pmod{\pi^8}$. Donc

$$a_6 \equiv \frac{1}{\pi^6}\frac{c_6'}{\varepsilon}\left(c_6'^2 - 3c_4' - 2\right) \pmod 2.$$

D'où la troisième congruence car $c_6'/\varepsilon \equiv 1 \pmod 2$. On en déduit

$$c_4' \equiv \pi^6 a_6 + \frac{1}{3}(c_6'^2 - 2) \pmod{\pi^8}.$$

Or, $1/3 \equiv -1 \pmod{2\pi}$ et $c_6'^2 - 1 \equiv 0 \pmod{4\pi}$ car $c_6' \equiv 1 \pmod 2$. Donc, $(c_6'^2 - 1)/3 \equiv 1 - c_6'^2 \pmod{\pi^8}$. Comme par ailleurs, $-1/3 \equiv 5 \pmod{\pi^8}$, on en déduit la dernière congruence et le lemme.

Proposition 3.53 *On a* $|\Phi| = 3$ *si et seulement si les conditions suivantes sont satisfaites*

1. *on a* $v(\Delta) \equiv 4 \pmod{12}$ *;*
2. *il existe* $(a, b) \in \mathcal{L}_1$ *tel que* $c_4' \equiv a \pmod{\pi^8}$ *et* $c_6' \equiv b \pmod{\pi^6}$.

Démonstration. Supposons $|\Phi| = 3$. D'après [Kra90, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 3.47, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. La première condition est donc satisfaite et d'après le lemme 3.48, on a $c_6' \equiv 1 \pmod 2$. De plus, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. D'après la proposition 3.50, le modèle (W) de E est entier. Exprimons à présent le fait que l'on n'est pas dans un cas 3 de Tate. On a $a_4 \equiv 1 \pmod 2$, donc $r = 1$ satisfait à la première relation de divisibilité de [Pap93, prop. 1].

Supposons $a_2 \equiv 1 \pmod \pi$. Alors, $t = 0$ satisfait à la seconde relation. Puis,

$$a_2 + a_6 \equiv a_6 + a_4 + a_2 + 1 \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([Pap93, prop. 1]).

Supposons $a_2 \equiv 0 \pmod \pi$. Alors, $t = 1$ satisfait à la seconde relation. Puis,

$$a_6 + a_4 + a_2 - \frac{2}{\pi} \equiv a_2 + a_6 + 1 + \pi \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([Pap93, prop. 1]). D'où $a_2 + a_6 \equiv 1 + \pi \pmod 2$. Autrement dit, on a $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod 2$. De plus, d'après le lemme 3.52, on a

$$c_6' \equiv \pi^2 a_2 - \varepsilon \pmod 4 \quad \text{et} \quad c_4' \equiv -c_6'^2 + 6 + \pi^6 a_6 \pmod{\pi^8}. \tag{3.29}$$

Par ailleurs, d'après la proposition 3.50 et les congruences $a_2 + a_6 \equiv 0$ ou $1+\pi \pmod 2$, on a

$$(a_2 \pmod 2, a_6 \pmod 2) \in \{(0, 1+\pi), (1,1), (\pi, 1), (1+\pi, 1+\pi)\}.$$

On déduit alors des congruences de la formule (3.29) les quatre couples ($c_4' + c_6'^2 \pmod{\pi^8}, c_6' \pmod 4$) possibles. À chaque classe $c_6' \pmod 4$ correspond quatre valeurs possibles pour $c_6' \pmod{\pi^6}$. En remplaçant $c_6'^2 \pmod{\pi^8}$ par sa valeur dans la seconde congruence de (3.29), on obtient ainsi les seize couples ($c_4' \pmod{\pi^8}, c_6' \pmod{\pi^6}$) de l'ensemble $\mathcal{L}_1$.

Réciproquement, supposons les conditions de l'énoncé satisfaites. Alors, on a $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 3.48, $v(\Delta_m) = 4$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. Alors, d'après l'appendice 3.5, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3 de Tate. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [Pap93, prop.1]. De plus, d'après le lemme 3.52, on a

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c_6' + 1) \pmod 2 \quad \text{et} \quad a_6 \equiv \frac{1}{\pi^6}(c_6'^2 - 3c_4' - 2) \pmod 2.$$

On vérifie alors que pour chacun des seize couples de l'ensemble $\mathcal{L}_1$, on a $a_2 + a_6 \equiv 0$ ou $1+\pi \pmod 2$.

Supposons $a_2 + a_6 \equiv 0 \pmod 2$. Alors, $t = 0$ satisfait à la seconde relation de divisilité de [Pap93, prop.1] et $a_6 + a_4 + a_2 + 1 \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_2 + a_6 \equiv 1 + \pi \pmod 2$, alors, $t = 1$ convient et $a_6 + a_4 + a_2 - 2/\pi \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4 de Tate. Par ailleurs, d'après le lemme 3.51, on n'est pas dans un cas 4 de Tate. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [Kra90, th.2(i)].

Cas où $v(j) = 16$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 16$ et la condition (C2), i.e. $j' \equiv 1 + \pi^2 \pmod{2\pi}$.

Lemme 3.54 *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV^*. Alors, on a $v(\Delta_m) = 8$.*

Démonstration. D'après [Kra90, th.2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. C'est en contradition avec la condition $v(j) = 16$. Par ailleurs, si E est de type IV^*, alors $v(\Delta_m) = 8$. D'où le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2} \quad \text{et} \quad a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3}.$$

Proposition 3.55 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. Alors, l'équation*

$$y^2 = x^3 + a_4 x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E. De plus, les coefficients a_4 et a_6 sont deux unités de $\mathcal{O}_K$ satisfaisant aux congruences suivantes :

$$a_4 \equiv c_4' \pmod 4, \quad a_6 \equiv \left(\frac{\pi^2}{2}\right) c_6' \pmod 4$$

et

$$a_4 \equiv 1 \pmod 2, \quad a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}.$$

Démonstration. Sous l'hypothèse $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, le modèle proposé n'est rien d'autre que le modèle (W_0) de E. En effet, on a

$$-\frac{c_4}{48} = -3\frac{c_4'}{\varepsilon^2} = a_4 \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} = a_6.$$

Les coefficients a_4 et a_6 sont deux unités de $\mathcal{O}_K$. De plus,

$$a_4 = -\frac{3}{\varepsilon^2}c_4' \equiv c_4' \pmod 4$$

et

$$a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} \equiv \left(\frac{\pi^2}{2}\right)c_6' \pmod 4$$

car $\varepsilon^2 \equiv 1 \pmod 4$. On a enfin

$$j' = \left(\frac{2}{\pi^2}\right)^8 \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

D'où $a_4^3 \equiv a_6^2 + \pi^2 \pmod{2\pi}$, d'après la condition (C2). Or, a_6 étant une unité de $\mathcal{O}_K$, on a $a_6^2 \equiv 1 \pmod 2$. D'où $a_4 \equiv 1 \pmod 2$ et $a_4^2 \equiv 1 \pmod 4$. D'où le résultat.

Lemme 3.56 *Supposons que E soit de type IV^*. Alors, $c_6' \equiv 2/\pi^2 \pmod 2$.*

Démonstration. D'après le lemme 3.54, on a $v(\Delta_m) = 8$. Donc, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On considère alors le modèle (W) de E de la proposition 3.55. On a $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv (\pi^2/2)c_6' \pmod 2$. D'après [Pap93, prop.1] appliquée à $r = t = 1$, on a alors, comme E correspond à un cas 8 de Tate,

$$0 \equiv a_6 + a_4 \equiv 1 + \left(\frac{\pi^2}{2}\right)c_6' \pmod 2.$$

D'où le résultat.

Lemme 3.57 *Supposons que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$ et $c_6' \equiv 2/\pi^2 \pmod 2$. Alors, la courbe E est de type IV^* si et seulement si $a_4 + a_6 \equiv 0$ ou $\pi^2 + \pi^3 \pmod 4$.*

Démonstration. D'après l'appendice 3.5, la courbe E correspond à un cas 3, 4, 6, 7 ou 8 (type IV^*) de Tate. Pour le modèle (W) de E de la proposition 3.55, on a, avec les notations de [Tat75],

$$b_2 = 0; \quad b_4 = 2a_4 = -\frac{6}{\varepsilon^2}c_4'; \quad b_6 = 4a_6 = -4\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3};$$

$$b_8 = -a_4^2 = -9\frac{c_4'^2}{\varepsilon^4}.$$

D'après les hypothèses faites et la proposition 3.55, on a $a_6 \equiv (\pi^2/2)c'_6 \equiv 1 \pmod 2$ et $a_4 \equiv 1 + \pi^2 \pmod{2\pi}$. Donc, d'après [Pap93, prop.1] appliqué à $r = t = 1$, on est dans un cas ≥ 4 de Tate. De plus, comme $\varepsilon \equiv \pm 1 \pmod 4$, on a

$$b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -9 - 4 - 18(1 + \pi^2) + 3 \equiv 0 \pmod{4\pi}.$$

Donc d'après [Pap93, prop.2] appliqué à $r = 1$, on est dans un cas ≥ 5 de Tate. Vérifions que l'on n'est jamais dans un cas 7 de Tate. En effet, d'après ce qui précède, $r = 1$ satisfait à la condition (a) de [Pap93, prop. 3] et $s = 1$ satisfait à la condition (b). D'où le fait que l'on n'est jamais dans un cas 7 de Tate. Autrement dit, on est dans un cas 8 de Tate si et seulement si on n'est pas dans un cas 6, c'est-à-dire, d'après [Pap93, prop.3(b)], si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 + a_4 + 1 \equiv t^2 \pmod 4$. Or, $a_6 + a_4 + 1$ étant une unité de $\mathcal{O}_K$, on en déduit que $t \in \mathcal{U}_K$ et on conclut avec le lemme 3.11.

Proposition 3.58 *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 8 \pmod{12}$;*
2. *il existe $(a, b) \in \mathcal{L}_2$ tel que $c'_4 \equiv a \pmod 4$ et $c'_6 \equiv b \pmod 4$.*

Démonstration. Supposons $|\Phi| = 3$. D'après [Kra90, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 3.54, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. D'après le lemme 3.56, on a de plus, $c'_6 \equiv 2/\pi^2 \pmod 2$. Donc d'après le lemme 3.57 on a $a_4 + a_6 \equiv 0$ ou $\pi^2 + \pi^3 \pmod 4$. Or, d'après la proposition 3.55, on a

$$a_4 + a_6 \equiv c'_4 + \left(\frac{\pi^2}{2}\right) c'_6 \pmod 4$$

On en déduit que l'on a, ou bien $c'_4 \equiv -(\pi^2/2)c'_6 \pmod 4$, ou bien, $c'_4 \equiv -(\pi^2/2)c'_6 + \pi^2 + \pi^3 \pmod 4$. En distinguant chaque fois selon les quatre valeurs possibles pour $c'_6 \pmod 4$, on obtient les huit couples $(c'_4 \pmod 4, c'_6 \pmod 4)$ possibles. On vérifie alors qu'il existe $(a, b) \in \mathcal{L}_2$ tel que a (resp. b) soit un représentant de c'_4 (resp. c'_6) modulo 4.

Réciproquement, si les deux conditions de l'énoncé sont satisfaites, alors d'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On vérifie de plus que l'on a nécessairement $c'_6 \equiv 2/\pi^2 \pmod 2$. D'après la proposition 3.55 et la seconde hypothèse, il vient alors :

$$a_4 + a_6 \equiv c'_4 + \left(\frac{\pi^2}{2}\right) c'_6 \equiv 0 \text{ ou } \pi^2 + \pi^3 \pmod 4$$

Donc d'après le lemme 3.57, E est de type IV^*. D'où $|\Phi| = 3$ d'après [Kra90, th.2(i)].

Cas où $v(j) = 20$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 20$ et la condition (C1'), i.e. $c'_4 \equiv 1 + \pi \pmod 2$.

Lemme 3.59 *La courbe E n'est pas de type IV^*. Supposons qu'elle soit de type IV. Alors, on a $v(\Delta_m) = 4$.*

Démonstration. D'après [Kra90, th.2(i)], si E est de type IV^*, on a $v(\Delta_m) = 8$. C'est en contradiction avec le condition $v(j) = 20$. Par ailleurs, si E est de type IV, alors $v(\Delta_m) = 4$. D'où le lemme.

Lemme 3.60 *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, on a $v(\Delta_m) = 4$ si et seulement si $c_6' \equiv \pi^2/2 \pmod 2$.*

Démonstration. Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, d'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (12, 14, 16).$$

Le modèle (W_0) de E est alors entier. D'après l'appendice 3.5, il correspond à un cas 10 de Tate ou à un cas non minimal. Examinons donc à quelle condition il est minimal. Avec les notations de [Tat75], on a, pour le modèle (W_0) de E :

$$b_6 = -4\frac{c_6}{864} = -2^3\pi^2\frac{c_6'}{\varepsilon^3}; \quad b_8 = -\left(\frac{c_4}{48}\right)^2.$$

En particulier, on a $v(b_8) = 8$, donc $r = 0$ satisfait à la condition de [Pap93, prop.6]. S'il existe un entier x de K tel que

$$b_6 \equiv x^2 \pmod{\pi^{10}},$$

alors on a nécessairement $v(x) = 4$, car $v(b_6) = 8$. Puis, il vient

$$c_6' \equiv \left(\frac{\pi^2}{2}\right)\left(\frac{x}{2\pi^2}\right)^2 \pmod 2.$$

D'où $c_6' \equiv \pi^2/2 \pmod 2$ car $x/2\pi^2 \in \mathcal{U}_K$.

Réciproquement, si l'on a $c_6' \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ convient. Avec [Pap93, prop.6], cela démontre le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2}; \qquad a_6 = -\frac{1}{\pi^2}\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c_6' + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right).$$

Proposition 3.61 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. Alors, l'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + a_4x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel on a $a_4 \equiv 1 + \pi \pmod 2$.

Démonstration. Le changement de variables

$$X = x; \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $4/\pi^3$ est entier. Vérifions que les coefficients a_4 et a_6 sont également entiers et que l'on a $a_4 \equiv 1+\pi \pmod 2$.

On a

$$a_4 = -3\frac{c_4'}{\varepsilon^2} \equiv -3(1+\pi) \equiv 1+\pi \pmod 2,$$

car $c_4' \equiv 1+\pi \pmod 2$ d'après la condition (C1').

D'après le lemme 3.60, on a $c_6' \equiv \pi^2/2 \pmod 2$. D'où

$$\pi^2 a_6 = -\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c_6' + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right) \equiv 0 \pmod 2,$$

car $\varepsilon \equiv 1 \pmod 2$ (lemme 3.14). D'où la proposition.

Lemme 3.62 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8,8,4)$. *Alors, E ne correspond pas à un cas 4 de Tate.*

Démonstration. D'après l'appendice 3.5, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 3.61. Supposons qu'il corresponde à un cas ≥ 4 de Tate. D'après la congruence $a_4 \equiv 1+\pi \pmod 2$, $r=1$ satisfait à la première relation de divisibilité de [Pap93, prop. 2]. On a par ailleurs, avec les notations de [Tat75],

$$b_2 = 0; \quad b_4 = -6\frac{c_4'}{\varepsilon^2} \equiv \pi^2 \pmod{2\pi}; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6 \equiv \pi^2 \pmod{2\pi};$$

$$b_8 = -9\frac{c_4'^2}{\varepsilon^4} \equiv -(1+\pi)^2 \equiv -(1+\pi^2) \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -(1+\pi^2) + 3\pi^2 + 3\pi^2 + 3 \equiv 0 \pmod{2\pi}$. D'où le résultat d'après [Pap93, prop. 2].

Lemme 3.63 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8,8,4)$. *Alors, a_6 est entier et l'on a les congruences*

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right)c_6'\right) \pmod 2 \quad \textit{et} \quad c_6' \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

Démonstration. Sous l'hypothèse faite, on a on a $c_6' \equiv \pi^2/2 \pmod 2$ et l'élément a_6 est entier. Comme $\varepsilon \equiv \pm 1 \pmod 4$, on a de plus,

$$-\pi^2 a_6 \equiv \left(\frac{2}{\pi^2}\right)\varepsilon c_6' + \left(\frac{2}{\pi^2}\right)^2 \equiv \left(\frac{2}{\pi^2}\right)^2\left(1 + 3\left(\frac{2}{\pi^2}\right)c_6'\right) \pmod 4.$$

Or, $(2/\pi^2)^2 \equiv 1 \pmod 2$ et $v(1+3(2/\pi^2)c_6') \geq 2$, d'où

$$\pi^2 a_6 \equiv 1 - \left(\frac{2}{\pi^2}\right)c_6' \pmod 4$$

et la première congruence. On en déduit alors la seconde car $\pi^4 \equiv 4 \pmod{\pi^6}$.

Proposition 3.64 *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 4 \pmod{12}$;*
2. *on a $c_6' \equiv \frac{\pi^2}{2} + 2 \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + \pi^3 \pmod 4$.*

Démonstration. Supposons $|\Phi| = 3$. D'après [Kra90, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 3.59, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. Donc, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. De plus, d'après le lemme 3.60, on a $c_6' \equiv \pi^2/2 \pmod 2$. Les coefficients a_4 et a_6 sont alors entiers d'après la proposition 3.61. Exprimons le fait que l'on n'est pas dans le cas 3 de Tate. On a $a_4 \equiv 1 \pmod \pi$, donc $r = 1$ satisfait à la première relation de divisibilité de [Pap93, prop.1].

Supposons $a_6 \equiv 1 \pmod \pi$. Alors, $t = 1$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 - \pi \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([Pap93, prop. 1]). Donc $a_6 \equiv 1 \pmod 2$ car $a_4 \equiv 1 + \pi \pmod 2$ d'après la proposition 3.61.

Supposons $a_6 \equiv 0 \pmod \pi$. Alors, $t = 0$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 + 1 \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([Pap93, prop. 1]). D'où $a_6 \equiv \pi \pmod 2$ car $a_4 \equiv 1 + \pi \pmod 2$ d'après la proposition 3.61. La troisième condition est donc satisfaite. Autrement dit, on a $a_6 \equiv 1$ ou $\pi \pmod 2$. Or, d'après le lemme 3.63, on a

$$c_6' \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

D'où la seconde condition.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, on a $c_6' \equiv \pi^2/2 \pmod 2$. D'après le lemme 3.60, on a donc $v(\Delta_m) = 4$ et on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. D'après l'appendice 3.5, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3 de Tate. On considère le modèle de E de la proposition 3.61. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [Pap93, prop.1].

Par ailleurs, d'après le lemme 3.63, on a

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right) c_6'\right) \pmod 2.$$

D'où, $a_6 \equiv 1$ ou $\pi \pmod 2$.

Supposons $a_6 \equiv 1 \pmod 2$. Alors, $t = 1$ satisfait à la seconde relation de divisilité de [Pap93, prop.1] et $a_4 + a_6 - \pi \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_6 \equiv \pi \pmod 2$, alors, $t = 0$ convient et $a_4 + a_6 + 1 \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4 de Tate. Par ailleurs, d'après le lemme 3.62, on n'est pas dans un cas 4 de Tate. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [Kra90, th.2(i)].

Cas où $v(j) \geq 24$

On suppose que le modèle de Weierstrass de E vérifie $v(j) \geq 24$ et que 3 ne divise pas $v(\Delta)$.

Lemme 3.65 *On suppose* $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. *Alors, E est de type IV^* si et seulement si on a* $c'_6 \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c'_6 \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Démonstration. On considère le modèle (W_0) de E. Sous l'hypothèse faite, ce modèle est entier et il correspond à un cas 3, 6 ou 8 (type IV^*) de Tate (d'après l'appendice 3.5). De plus, on a

$$-\frac{c_4}{48} = -\frac{3}{\varepsilon^2}\pi^{v(c_4)-8}c'_4 \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c'_6}{\varepsilon^3}. \tag{3.30}$$

Les deux premières relations de congruence de [Pap93, prop.1] sont satisfaites par $r = 0$ et $t = 1$, puis

$$-\frac{c_6}{864} - 1 \equiv \left(\frac{2}{\pi^2}\right)c'_6 - 1 \pmod 2.$$

Autrement dit, on est dans un cas ≥ 4 si et seulement si $c'_6 \equiv \pi^2/2 \pmod 2$. Avec les notations de [Tat75], on a $b_8 = -(c_4/48)^2$, donc $v(b_8) \geq 6$ et $r = 0$ satisfait la condition (a) de [Pap93, prop.3]. On conclut alors que E est de type IV^* si et seulement si il existe t dans $\mathcal{O}_K$ tel que $-c_6/864 \equiv t^2 \pmod 4$. D'après le lemme 3.11 et la seconde égalité (3.30), c'est le cas si et seulement si $c'_6 \equiv \frac{\pi^2}{2} \pmod 4$ ou $c'_6 \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$. D'où le lemme.

Lemme 3.66 *On suppose* $v(\Delta) \equiv 4 \pmod{12}$. *Alors, on a* $v(\Delta_m) = 4$ *si et seulement si* $c'_6 \equiv \frac{\pi^2}{2} \pmod 2$.

Démonstration. D'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 14, 14, 16)$. Le modèle (W_0) de E est alors entier. De plus, on a $v(\Delta_m) = 4$ si et seulement si ce modèle est non minimal, c'est-à-dire, toujours d'après l'appendice 3.5, si et seulement si il ne correspond pas à un cas 10 de Tate. Avec les notations de [Tat75], on a $b_8 = -(c_4/48)^2$ et $v(c_4/48) \geq 6$, donc $v(b_8) \geq 12$. On en déduit que $r = 0$ satisfait la première relation de congruence de [Pap93, prop.6]. Par ailleurs, pour ce modèle, on a $b_6 = -4c_6/864 = -8\pi^2 c'_6/\varepsilon^3$. Puis, le modèle (W_0) est non minimal si et seulement si il existe x dans $\mathcal{O}_K$ tel que

$$-8\pi^2\frac{c'_6}{\varepsilon^3} \equiv x^2 \pmod{\pi^{10}}.$$

Autrement dit, si et seulement si il existe x dans $\mathcal{O}_K$ tel que $8\pi^2 c'_6 \equiv x^2 \pmod{\pi^{10}}$. Comme c'_6 est une unité de $\mathcal{O}_K$, si un tel x existe, on a nécessairement $v(x) = 4$ et la congruence ci-dessus équivaut à $c'_6 \equiv (\pi^2/2)(x/2\pi^2)^2 \pmod 2$, puis $c'_6 \equiv \pi^2/2 \pmod 2$ d'après le lemme 3.11. Réciproquement, si $c'_6 \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ satisfait à la congruence ci-dessus. Cela démontre le lemme.

Posons

$$a_4 = -3\frac{c'_4}{\varepsilon^2}\pi^{v(c_4)-8}; \qquad a_6 = -\frac{1}{\pi^6}\left(4 + 2\pi^2\frac{c'_6}{\varepsilon^3}\right).$$

Proposition 3.67 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, l'équation*

$$y^2 + \frac{4}{\pi^3} y = x^3 + a_4 x + a_6, \qquad (W)$$

définit un modèle de Weierstrass entier de E.

Démonstration. Le changement de variables

$$X = x; \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition. Les coefficients $4/\pi^3$ et a_4 sont entiers. Vérifions que c'est également le cas pour a_6. D'après le lemme 3.66, on a $c_6' \equiv \frac{\pi^2}{2} \pmod 2$. Puis,

$$-\pi^6 a_6 = 4 + 2\pi^2 \frac{c_6'}{\varepsilon^3} \equiv 4 + 2\pi^2 c_6' \pmod{\pi^6}.$$

Comme $4 \equiv \pi^4 \pmod{\pi^6}$, on a donc $-\pi^6 a_6 \equiv 0 \pmod{\pi^6}$ et a_6 est entier. D'où la proposition.

Lemme 3.68 *On suppose* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, E est de type IV si et seulement si on a* $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Démonstration. On considère alors le modèle (W) de E de la proposition 3.67. Il correspond, d'après l'appendice 3.5, à un cas 3 ou 5 (type IV) de Tate. Comme $v(a_4) \geq 2$ (car $v(c_4) \geq 10$), $r = 0$ satisfait à la première relation de congruence de [Pap93, prop.1]. On est donc dans un cas 5 de Tate si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 \equiv t^2 + t\pi \pmod 2$, autrement dit, si et seulement si $a_6 \equiv 0$ ou $1 + \pi \pmod 2$. Or, comme $-\pi^6 a_6 \equiv 4 + 2\pi^2 \varepsilon c_6' \pmod{\pi^8}$, la congruence $a_6 \equiv 0 \pmod 2$ équivaut à $c_6' \equiv -\frac{4}{2\pi^2\varepsilon} \equiv \pi^2/2 \pmod 4$. De même, $a_6 \equiv 1 + \pi \pmod 2$ équivaut à $c_6' \equiv -\frac{4}{2\pi^2\varepsilon} + \frac{\pi^6}{2\pi^2\varepsilon} + \frac{\pi^7}{2\pi^2\varepsilon} \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$. D'où le lemme.

Proposition 3.69 *On a* $|\Phi| = 3$ *si et seulement si les deux conditions suivantes sont satisfaites*

1. *on a* $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$;
2. *on a* $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Démonstration. On suppose que l'on a $|\Phi| = 3$. Alors, d'après [Kra90], E est de type IV ou IV^*. Supposons qu'elle soit de type IV. Dans ce cas, $v(\Delta_m) = 4$ et quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. Puis d'après le lemme 3.68, on a $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$. D'où la première condition de l'énoncé. De même, si la courbe E est de type IV^*, alors, d'après [Kra90], on a $v(\Delta_m) = 8$ et quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. D'après le lemme 3.65, on a donc $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Réciproquement, supposons que les deux conditions de l'énoncé soient satisfaites. Si $v(\Delta) \equiv 4 \pmod{12}$, comme $c_6' \equiv \pi^2/2 \pmod 2$, on a $v(\Delta_m) = 4$ d'après le lemme 3.66. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. On conclut avec le lemme 3.68 que la courbe E est de type IV. De même, si $v(\Delta) \equiv 8 \pmod{12}$, alors d'après l'appendice 3.5, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$ et on conclut que la courbe E est de type IV^* avec le lemme 3.65. Autrement dit, E est de type IV ou IV^* et $|\Phi| = 3$ d'après [Kra90, th.2]. D'où la proposition.

3.4 Annexe A – Exemples

On montre dans cet appendice que tous les cas du théorème 3.2 se réalisent. C'est immédiat pour les assertions 1, 2 et 3 en raison de l'existence d'une courbe elliptique sur K d'invariant j donné. On adopte dans toute cette section les notations de [Tat75].

3.4.1 Cas où $v(j) \geq 24$

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{13}}{48}x - \frac{\pi^{12}}{864}$$

vérifie $v(j) = 27$ et $v(\Delta) = 12$. D'après le théorème 3.2, on a $|\Phi| = 2$ et le cas $11(a)$ se réalise.

Vérifions qu'il en va de même du cas $11(b)$. La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{11}}{48}x - \frac{\pi^{10}a}{864}, \quad \text{avec } a \in \mathcal{U}_K,$$

vérifie $v(j) = 25$ et $v(\Delta) = 8$. D'après le théorème 3.2, on a donc

$$|\Phi| = \begin{cases} 3 & \text{si } a \equiv 2/\pi^2 \pmod 4 \text{ ou } a \equiv 2/\pi^2 + 2 + \pi^3 \pmod 4 \\ 6 & \text{sinon.} \end{cases}$$

et le cas $11(b)$ se réalise également.

3.4.2 Cas où $v(j) = 16$, 18 et 20

Pour $i = 16$, 18 ou 20, l'équation

$$y^2 + \pi^2 xy = x^3 - \frac{36\pi^8}{\pi^i - 1728}x - \frac{\pi^{12}}{\pi^i - 1728} \tag{3.31}$$

définit un modèle entier d'une courbe elliptique sur K d'invariant modulaire $j = \pi^i$. En particulier, on a $j' = 1$. De plus, on a

$$\begin{aligned} c_4 = \pi^8 + \frac{1728\pi^8}{\pi^i - 1728} &= \pi^8 \left(1 - \frac{1}{1 - \frac{\pi^i}{1728}}\right) \\ &= \frac{\pi^{8+i}}{1728}\left(1 + \sum_{k\geq 1}\left(\frac{\pi^i}{1728}\right)^k\right). \end{aligned}$$

Donc, en particulier, $v(c_4) = 8 + i - 12$ et $c'_4 \equiv \frac{\pi^{12}}{3^3 \cdot 2^6} \equiv 1/\varepsilon^3 \equiv 1 \pmod 2$. Autrement dit, la courbe ci-dessus ne vérifie ni la condition (C1'), ni la condition (C2). Cela démontre que les cas $8(b)$ et $10(b)$ du théorème 3.2 se réalisent.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{12}(1+\pi)}{48}x - \frac{\pi^{15}}{864} \tag{3.32}$$

vérifie $v(j) = 18$ et $c'_4 = 1 + \pi$. La condition (C1') est donc vérifiée. Avec l'exemple précédent pour $i = 18$, cela montre que le cas 9 se réalise également.

Cas où $v(j) = 16$ et la condition (C2) est vérifiée

On commence par démontrer le résultat suivant.

Proposition 3.70 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 = x^3 + a_4 x + a_6,$$

avec a_4 et a_6 deux unités vérifiant $a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}$. Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8) \quad \textit{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

Démonstration. On a $b_2 = 0$, $b_4 = 2a_4$, $b_6 = 4a_6$ et $b_8 = -a_4^2$. Donc,

$$c_4 = -48a_4, \quad c_6 = -864a_6 \quad \text{et} \quad \Delta = -16(4a_4^3 + 27a_6^2).$$

Comme a_4 et a_6 sont deux unités de $\mathcal{O}_K$, on a, en particulier, $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. De plus, on a

$$j' = \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

Or, $a_4^2 \equiv 1 \pmod{2\pi}$, car $a_4 \equiv a_6^2 \pmod 2$. D'où, $j' \equiv a_4/a_6^2 \equiv 1 + \pi^2 \pmod{2\pi}$. Cela démontre la proposition.

Exemple 3.71 *La courbe E d'équation*

$$y^2 = x^3 - x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, la condition (C2) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.70. De plus, on a

$$c'_4 = \frac{48}{\pi^8} = \frac{1}{3}\varepsilon^2 \equiv -1 \pmod 4 \quad \text{et} \quad c'_6 = -\frac{864}{\pi^{10}} = -\frac{2^5 \cdot 3^3}{\pi^{10}} \equiv \frac{2}{\pi^2} \pmod 4.$$

Le couple $(-1, 2/\pi^2) \in \mathcal{L}_2$ est alors un représentant modulo 4 du couple $(c'_4 \pmod 4, c'_6 \pmod 4)$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 8 du théorème 3.2.

Exemple 3.72 *La courbe E d'équation*

$$y^2 = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$*, la condition (C2) et* $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.70. De plus, on a

$$c_6' = -\frac{864}{\pi^{10}}(1+\pi) \equiv \frac{2}{\pi^2} + \pi \pmod 2.$$

En particulier, il n'existe aucun couple (a, b) de $\mathcal{L}_2$ tel que $c_6' \equiv b \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 8 du théorème 3.2.

Cela démontre que tous les cas de l'assertion 8 se réalisent.

Cas où $v(j) = 20$ et la condition (C1') est vérifiée

On commence par démontrer le résultat suivant.

Proposition 3.73 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{4}{\pi^3}y = x^3 + a_4 x + a_6,$$

avec $a_4 \equiv 1 + \pi \pmod 2$*. Alors, on a*

$$(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4) \quad \textit{et} \quad c_4' \equiv 1 + \pi \pmod 2.$$

Démonstration. On a $b_4 = 2a_4$ et donc $v(b_4) = 2$. On en déduit que $c_4 = -24b_4$ vérifie $v(c_4) = 8$, puis $c_4' = -\frac{2^4 \cdot 3}{\pi^8} a_4 = -3\left(\frac{2}{\pi^2}\right)^4 a_4 \equiv 1 + \pi \pmod 2$. De même, on a $b_6 = (4/\pi^3)^2 + 4a_6$ et donc $v(b_6) = 2$. D'où, $c_6 = -216b_6$ vérifie $v(c_6) = 8$. Enfin, $\Delta = -8b_4^3 - 27b_6^2$ vérifie $v(\Delta) = 4$. D'où la proposition.

Exemple 3.74 *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + (1+\pi)x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$*, la condition (C1') et* $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.73. De plus, on a

$$c_6' = -\frac{432}{\pi^8}\left(2 + \frac{8}{\pi^6}\right) \equiv 2 + \frac{8}{\pi^6} \equiv \frac{\pi^2}{2} + 2 \pmod 4.$$

On conclut que l'on a $|\Phi| = 3$ avec l'assertion 10 du théorème 3.2.

Exemple 3.75 *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + (1+\pi)x$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$*, la condition (C1') et* $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.73. De plus, on a

$$c_6' = -\frac{3456}{\pi^6} \equiv -\frac{1}{3}\left(\frac{\pi^2}{2}\right)\varepsilon^4 \equiv \frac{\pi^2}{2} \pmod 4.$$

On conclut que l'on a $|\Phi| = 6$ avec l'assertion 10 du théorème 3.2.

Cela démontre que tous les cas de l'assertion 10 se réalisent.

3.4.3 Cas où $v(j) = 12$

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{14}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4)+1$. Cela montre que le cas 7a du théorème 3.2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{16}}{864}, \quad \text{où } a \in \mathcal{U}_K$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4) + 2$. Elle vérifie la condition (C1') si et seulement si $a \equiv 1 + \pi \pmod 2$. Elle vérifie la condition (C3) si et seulement si on a $a \equiv 1 + \pi^2 \pmod 4$ ou $a \equiv 1 + \pi^3 \pmod 4$. Cela montre que le cas 7b du théorème 3.2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{15}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4)+3$. Cela montre que le cas 7c du théorème 3.2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{17}}{864}, \quad \text{où } a \in \mathcal{U}_K$$

vérifie $v(j) = 12$, $v(c_4) = 10$ et $2v(c_6) - 3v(c_4) = 4$. Elle vérifie la condition (C3) si et seulement si on a $a \equiv 1 + \pi^2 \pmod 4$ ou $a \equiv 1 + \pi^3 \pmod 4$. Cela montre que le cas 7d du théorème 3.2 se réalise.

Cela démontre que tous les cas de l'assertion 7 se réalisent.

3.4.4 Cas où $v(j) = 4$, 6 ou 8

On considère la courbe $\widetilde{E}$ d'équation (3.2) déduite de la courbe d'équation (3.31). Elle vérifie $v(j) = 24 - i$, où $i = 16$, 18 ou 20, c'est-à-dire $v(j) = 4$, 6 ou 8. Ses invariants standard sont notés $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ et satisfont d'après le lemme 3.27 aux congruences suivantes :

$$\widetilde{\Delta} \equiv c_4' \pmod 2 \quad \text{et} \quad \widetilde{j'} \equiv 1 \pmod 4.$$

En particulier, $\widetilde{E}$ ne vérifie ni la condition (C1), ni la condition (C2). Cela démontre que les cas $4(b)$ et $6(b)$ du théorème 3.2 se réalisent.

De même, la courbe $\widetilde{E}$ d'équation (3.2) déduite de la courbe d'équation (3.32) vérifie $v(j) = 6$ et la condition (C1). Avec l'exemple précédent, cela montre que le cas 5 se réalise également.

Cas où $v(j) = 4$ et la condition (C1) est vérifiée

On commence par démontrer le résultat suivant qui est une réciproque partielle à la proposition 3.42.

Proposition 3.76 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4 \quad \textit{et} \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8), \quad c_6' \equiv 1 \pmod 2 \quad \textit{et} \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration. On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = \frac{2^3}{\pi^4} + 2a_4; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6;$$

$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2$$

On en déduit, avec la définition de ε, que l'on a

$$b_2 = \frac{\pi^2}{3}\varepsilon + 4a_2; \quad b_4 = \frac{2}{3}\varepsilon + 2a_4; \quad b_6 = \frac{\pi^2}{9}\varepsilon^2 + 4a_6$$

et

$$b_8 = \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2.$$

En utilisant les congruences $a_2 \equiv a_6 \pmod 2$ et $a_4 \equiv \varepsilon \pmod{2\pi}$, il vient alors

$$v(b_2) = 2, \quad v(b_4) \geq 5, \quad v(b_6) = 2 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c_6' \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c_6' \equiv 1 \pmod 2$.

Il reste donc à montrer que l'on a, d'une part $v(\Delta) = 8$ et, d'autre part $\Delta' \equiv 1 + \pi \pmod 2$. C'est équivalent à montrer $\Delta \equiv \pi^8 + \pi^9 \pmod{\pi^{10}}$. On utilise pour ce faire les congruences suivantes que l'on démontre ci-dessous.

$$b_2^2 \equiv \pi^4 + 2\pi^6 a_2 + \pi^8 a_2^2 \pmod{\pi^{10}} \tag{3.33}$$

$$-27b_6^2 \equiv \pi^4 + \pi^8 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}} \tag{3.34}$$

$$b_8 \equiv 1 + \pi^5 + 4a_2^2 + 2\pi^2 a_2 \pmod{\pi^6} \tag{3.35}$$

$$9b_2b_4b_6 \equiv 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}. \tag{3.36}$$

D'après les égalités précédentes, on a

$$b_2^2 = \frac{\pi^4}{9}\varepsilon^2 + 16a_2^2 + 8\frac{\pi^2}{3}\varepsilon a_2.$$

Or, on a $\varepsilon^2/9 \equiv 1 \pmod{\pi^6}$, $4 \equiv \pi^4 \pmod{\pi^6}$ et $16 \equiv \pi^8 \pmod{\pi^{10}}$. Cela démontre la congruence (3.33). Pour les mêmes raisons, on a

$$b_6^2 = \frac{\pi^4}{3^4}\varepsilon^4 + 16a_6^2 + 8\frac{\pi^2}{9}\varepsilon a_6 \equiv \pi^4 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}}.$$

Puis, $-27 \equiv -3 \equiv 1 + \pi^4 \pmod{\pi^6}$. D'où la congruence (3.34).

Montrons à présent la congruence (3.35). On a

$$\begin{aligned} b_8 &= \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2 \\ &\equiv -\pi^2\varepsilon a_6 + 2\varepsilon a_4 + 4a_2a_6 + \pi^2 a_2 - a_4^2 \pmod{\pi^6}. \end{aligned}$$

Or, $a_2 + \varepsilon a_6 \equiv \pi^3 \pmod 4$ et $a_4 \equiv \varepsilon \pmod{2\pi}$. En particulier, $-a_4^2 \equiv 1 - 2\varepsilon a_4 \pmod{\pi^6}$ car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$. On en déduit donc que l'on a

$$b_8 \equiv \pi^2(2a_2 + \pi^3) + 1 + 4a_2^2 \equiv 1 + \pi^5 + 4a_2^2 + 2\pi^2 a_2 \pmod{\pi^6}.$$

Enfin, on a $b_2 \equiv b_6 \equiv \pi^2 \pmod{\pi^6}$ et $b_4 \equiv 2(a_4 - \varepsilon) \pmod{\pi^6}$. On en déduit alors la congruence (3.36).

Déduisons alors des congruences (3.33)-(3.36) celle annoncée pour Δ. On a

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

D'après les congruences (3.33) et (3.34) et l'hypothèse $a_2 \equiv a_6 \pmod 2$, on a

$$-27b_6^2 \equiv b_2^2 + \pi^8 \pmod{\pi^{10}}.$$

Comme $v(8b_4^3) \geq 10$, on a, d'après la congruence (3.36) et l'égalité ci-dessus

$$\Delta \equiv b_2^2(1 - b_8) + \pi^8 + 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}.$$

D'après les congruences (3.33) et (3.35), il vient alors

$$\Delta \equiv \pi^8 + \pi^9 + 4\pi^4 a_2^2 + 2\pi^6 a_2 + 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}.$$

Or, d'après la congruence de l'énoncé, $a_4 - \varepsilon \equiv \pi^2 a_2^2 + 2a_2 \pmod 4$, on a $+2\pi^4(a_4 - \varepsilon) \equiv 4\pi^4 a_2^2 + 2\pi^6 a_2 \pmod{\pi^{10}}$. En remplaçant dans la congruence ci-dessus, on obtient alors

$$\Delta \equiv \pi^8 + \pi^9 \pmod{\pi^{10}},$$

ce qui était le résultat cherché. Cela achève de démontrer la proposition 3.76.

Exemple 3.77 *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 - x^2 + (1 + \pi^3)x + 1 + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.76. De plus, on a

$$c_6' = -37\frac{2^6}{\pi^{12}} - 3\cdot 5\frac{2^6}{\pi^{10}} + 3\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c_6' \equiv \varepsilon + 2 + \pi^2 \pmod 4$. Or, comme K est dans Ω_1, on a $c_6' \equiv 1 + \pi^3 \pmod 4$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 4 du théorème 3.2.

Exemple 3.78 *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + x + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.76. De plus, on a

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon + 2 \pmod 4.$$

Or, comme K est dans Ω_1, on a $c_6' \equiv 1 + \pi^2 + \pi^3 \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 4 du théorème 3.2.

Exemple 3.79 *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 - x + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.76. De plus, on a

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon + 2 \pmod 4.$$

Or, comme K est dans Ω_2, on a $c_6' \equiv 1 \pmod 4$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 4 du théorème 3.2.

Exemple 3.80 *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + x^2 - x + 1 + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.76. De plus, on a

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3\cdot 5\frac{2^6}{\pi^{10}} - 3\cdot 5\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c_6' \equiv \varepsilon + 2 + \pi^2 \pmod 4$. Or, comme K est dans Ω_2, on a $c_6' \equiv 1 + \pi^2 \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 4 du théorème 3.2.

Cela démontre que tous les cas de l'assertion 4 se réalisent.

Cas où $v(j) = 8$ et la condition (C2) est vérifiée

On commence par démontrer le résultat suivant.

Proposition 3.81 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv 1 \pmod \pi$. Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4), \quad c'_6 \equiv 1 \pmod 2 \quad \textit{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

Démonstration. On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = 2a_4; \quad b_6 = 4a_6; \quad b_8 = \left(\frac{2}{\pi}\right)^2 a_6 + 4a_2a_6 - a_4^2.$$

En particulier, il vient

$$v(b_2) = 2, \quad v(b_4) = 2, \quad v(b_6) = 4 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c'_6 \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c'_6 \equiv 1 \pmod 2$.

Enfin, on a $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$. Donc, en particulier, $v(\Delta) = 4$ et on a

$$j' = \frac{c_4'^3}{\Delta'} \equiv -\frac{1}{b_8} \equiv -\frac{1}{\pi^2 - a_4^2} \pmod{2\pi}.$$

Or, $a_4 \equiv 1 \pmod 2$, donc $a_4^2 \equiv 1 \pmod{2\pi}$ et $j' \equiv 1 + \pi^2 \pmod{2\pi}$. D'où la proposition 3.81.

Exemple 3.82 *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$, la condition (C2) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.81. De plus, on a

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même, on a

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6} - 3^3\frac{2^5}{\pi^5}.$$

D'où, $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 + \pi^5 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors, on a

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8}$$

et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^4 \pmod{\pi^6}.$$

Autrement dit, le couple $(a,b) = (-\varepsilon^2+2\pi^4+6+\pi^6+\pi^7, -\varepsilon+\pi^4)$ de l'ensemble $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 6 du théorème 3.2.

Supposons alors $K \in \Omega_2$. Alors, on a

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 6 + 2\pi^4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8}$$

et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^5 \pmod{\pi^6}.$$

Autrement dit, le couple $(a,b) = (-\varepsilon^2 + 6 + \pi^6, -\varepsilon + \pi^5)$ de l'ensemble $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 6 du théorème 3.2 dans ce cas également. D'où le résultat en général.

Exemple 3.83 *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4,6,4)$, la condition (C2) et $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 3.81. De plus, on a

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même, on a

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6}.$$

D'où, $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 \equiv 5\varepsilon + 2 + 2\pi^2 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon + \pi^4 + \pi^5 \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a,b) de l'ensemble $\mathcal{L}_1$ vérifiant $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 6 du théorème 3.2.

Supposons alors $K \in \Omega_2$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a,b) de l'ensemble $\mathcal{L}_1$ vérifiant $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 6 du théorème 3.2 dans ce cas également. D'où le résultat en général.

Cela démontre que tous les cas de l'assertion 6 se réalisent.

3.5 Annexe B – Tableaux de Papadopoulos

On explicite dans cet appendice le Tableau V de [Pap93] dans le cas où, avec ses notations, $\lambda = 2$ (i.e. $e = 2$).

Type de Néron	II								
Cas de Tate	3								
$v(c_4)$	4	≥ 8	≥ 8	4	8	8	4	8	≥ 9
$v(c_6)$	6	8	10	6	11	≥ 12	6	12	11
$v(\Delta)$	4	4	8	6	10	12	7	13	10
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	4	4	8	6	10	12	7	13	10

Type de Néron	III									
Cas de Tate	4									
$v(c_4)$	4	8	8	4	8	9	9	9	9	9
$v(c_6)$	6	8	10	6	11	8	10	12	13	≥ 14
$v(\Delta)$	4	4	8	6	10	4	8	12	14	15
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	3	7	5	9	3	7	11	13	14

Type de Néron	IV		
Cas de Tate	5		
$v(c_4)$	4	8	≥ 10
$v(c_6)$	6	8	8
$v(\Delta)$	4	4	4
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	I_0^*								
Cas de Tate	6								
$v(c_4)$	8	4	8	8	4	8	≥ 10	≥ 10	≥ 10
$v(c_6)$	10	6	≥ 12	12	6	12	10	12	13
$v(\Delta)$	8	8	12	14	9	15	8	12	14
Conditions sup.	$*$	$*$	$*$	$*$			$*$	$*$	
$v(N)$	4	4	8	10	5	11	4	8	10

Type de Néron	I_1^*			I_3^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	10	10	6	≥ 12	12
$v(\Delta)$	8	8	8	11	12	12
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	3	3	3	4	5	5

Type de Néron	I_5^*			I_7^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	12	14	6	12	15
$v(\Delta)$	13	16	16	15	19	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	4	7	7	4	8	9

Type de Néron	I_2^*							
Cas de Tate	7							
$v(c_4)$	8	8	8	4	10	10	10	10
$v(c_6)$	≥ 12	12	12	6	12	14	≥ 15	15
$v(\Delta)$	12	14	16	10	12	16	18	19
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	6	8	10	4	6	10	12	13

Type de Néron	I_4^*					
Cas de Tate	7					
$v(c_4)$	8	8	4	10	10	10
$v(c_6)$	12	12	6	14	≥ 15	15
$v(\Delta)$	16	17	12	16	18	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	8	9	4	8	10	12

Type de Néron	I_6^*			
Cas de Tate	7			
$v(c_4)$	4	8	10	10
$v(c_6)$	6	12	15	15
$v(\Delta)$	14	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$
$v(N)$	4	8	10	11

Type de Néron	I_ν^*, $\nu \geq 8$		
Cas de Tate	7		
$v(c_4)$	4	8	10
$v(c_6)$	6	12	15
$v(\Delta)$	$8+\nu$	$12+\nu$	$14+\nu$
Conditions sup.	$*$	$*$	$*$
$v(N)$	4	8	10

On notera à cet endroit que si $\big(v(c_4), v(c_6), v(\Delta)\big)$ est le triplet $\big(10, 15, 14+\nu\big)$ et si ν est impair ≥ 9, Papadopoulos ne donne pas de condition supplémentaire $*$, mais il en existe une pour ce triplet si ν est pair ≥ 8.

Type de Néron	IV^*		
Cas de Tate	8		
$v(c_4)$	4	8	≥ 11
$v(c_6)$	6	10	10
$v(\Delta)$	8	8	8
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	III^*							
Cas de Tate	9							
$v(c_4)$	4	8	8	11	11	11	11	11
$v(c_6)$	6	12	≥ 12	12	14	15	16	≥ 17
$v(\Delta)$	10	14	12	12	16	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	7	5	5	9	11	13	14

Type de Néron	II*						
Cas de Tate	10						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	15	12	14	≥ 12	6	12	12
$v(\Delta)$	18	12	16	12	11	17	16
Conditions sup.		*	*	*	*	*	*
$v(N)$	10	4	8	4	3	9	8

Type de Néron	Équation non minimale						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	≥ 16	12	14	≥ 12	6	12	12
$v(\Delta)$	≥ 20	12	16	12	≥ 12	16	≥ 18
Conditions sup.		*	*	*	*	*	*

3.6 Annexe C – Le cas de $\mathbf{Q}_2$

Dans cette annexe, on explicite le groupe Φ dans le cas où $K = \mathbf{Q}_2$ en termes de la valuation de l'invariant modulaire j (autant qu'il est possible). Cette étude a déjà été menée par Kraus ([Kra90, Cor.]) et Cali ([Cal04]). L'énoncé ci-dessous ne diffère donc des précédents que dans sa formulation (à ceci près qu'on ne suppose pas le modèle minimal).

Théorème 3.84 *On suppose $K = \mathbf{Q}_2$. On est dans l'un des cas suivants.*

1. *Si $v(j) = 0$, on a $|\Phi| = 2$.*
2. *Si $v(j) \in \{1, 2, 5, 7, 10, 11\}$, on a $|\Phi| = 24$.*
3. *Si $v(j) \in \{3, 9\}$, on a $|\Phi| = 8$.*
4. *Supposons $v(j) = 4$.*
   (a) *Supposons $\Delta' \equiv -1 \pmod 4$. Alors*
   $$|\Phi| = \begin{cases} 3 & \text{si } c_6' \equiv -1 \pmod 4 \text{ et } v(\Delta) \equiv 8 \pmod{12}, \\ 6 & \text{sinon.} \end{cases}$$
   (b) *Supposons $\Delta' \equiv 1 \pmod 4$. Alors $|\Phi| = 24$.*
5. *Supposons $v(j) = 6$.*
   (a) *Si $2v(c_6) = 3v(c_4) + 1$, on a $|\Phi| = 4$.*
   (b) *Si $2v(c_6) > 3v(c_4) + 1$, on a $|\Phi| = 8$.*
6. *Supposons $v(j) = 8$.*
   (a) *Supposons $c_4' \equiv -1 \pmod 4$. Alors*
   $$|\Phi| = \begin{cases} 3 & \text{si } c_6' \equiv 1 \pmod 4 \text{ et } v(\Delta) \equiv 4 \pmod{12}, \\ 6 & \text{sinon.} \end{cases}$$

(b) *Supposons* $c_4' \equiv 1 \pmod 4$. *Alors* $|\Phi| = 24$.

7. *Supposons* $v(j) \geq 12$.

(a) *Si* 3 *divise* $v(\Delta)$, *on a* $|\Phi| = 2$.

(b) *Supposons que* 3 *ne divise pas* $v(\Delta)$. *On a*

$$|\Phi| = \begin{cases} 3 & \text{si } c_6' \equiv 1 \pmod 4 \text{ et } v(\Delta) \equiv 4 \text{ ou } 8 \pmod{12}, \\ 6 & \text{sinon.} \end{cases}$$

Chapitre 4

Critères d'irréductibilité pour les représentations des courbes elliptiques

Introduction

Soient $\overline{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et K un corps de nombres contenu dans $\overline{\mathbf{Q}}$. Étant donnés une courbe elliptique E définie sur K et un nombre premier p, on note $E[p]$ le groupe des points de p-torsion de la courbe E. C'est un espace vectoriel de dimension 2 sur le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ muni d'une action du groupe de Galois $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Cela fournit un homomorphisme

$$\rho_p : \mathrm{G}_K \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p).$$

Serre a démontré ([Ser72]) que pour toute courbe elliptique E/K sans multiplication complexe sur $\overline{\mathbf{Q}}$, il existe une constante $c(E,K)$ telle que pour tout nombre premier $p > c(E,K)$, la représentation ρ_p est *surjective*. Il a également posé la question (toujours ouverte, y compris pour $K = \mathbf{Q}$) de savoir si $c(E,K)$ peut être choisie indépendamment de E ([Ser79]).

Étant donnée une courbe E, on dit qu'un nombre premier p est *exceptionnel* si la représentation ρ_p est *réductible*. Si la courbe E est sans multiplication complexe, la finitude de l'ensemble des premiers exceptionnels résulte du théorème de Shafarevich ([Sil92, p.265] ou §4.2.1). Sur un corps K fixé, il n'y a qu'un nombre fini de classes de $\overline{\mathbf{Q}}$-isomorphismes de courbes elliptiques à multiplications complexes définies sur K. Par ailleurs, étant donnée une courbe à multiplications complexes définie sur K, l'ensemble des premiers exceptionnels peut être fini ou infini. Par exemple, la représentation ρ_p de la courbe définie sur $K = \mathbf{Q}(\sqrt{-3})$ par l'équation $y^2 = x^3 + 1$, est réductible pour tout nombre premier $p \equiv 1 \pmod 3$ (*c.f.* §4.6, ex. 4.36). Dans ce travail, on s'intéresse notamment à la question suivante.

Question 1. Le corps K et la courbe E étant donnés, peut-on décider en toute généralité si l'ensemble des nombres premiers exceptionnels est fini et si tel est le cas comment le déterminer explicitement ?

Lorsque E est sans multiplication complexe, Masser et Wüstholz ([MW93]), puis Pellarin ([Pel01]) ont obtenu des estimations de la constante $c(E,K)$ comme conséquence de leurs travaux sur le théorème d'isogénie. Ces résultats ne se prêtent cependant pas à une détermination explicite de l'ensemble des nombres premiers exceptionnels. En utilisant des arguments de théorie du corps de classes, on obtient un critère (théorème 4.1) portant sur la réduction de E en chaque place finie de K permettant d'aborder la question 1. On montre notamment que pour *toute* courbe elliptique définie sur un corps de degré *impair*, l'ensemble des nombres premiers exceptionnels est *fini* et qu'il est inclus dans l'ensemble des diviseurs premiers d'une collection explicite d'entiers (corollaire 4.3).

Ce critère est illustré numériquement dans le §4.6 où l'on détermine explicitement l'ensemble des nombres premiers exceptionnels de plusieurs courbes elliptiques (notamment sur des corps quadratiques).

On s'intéresse également dans ce travail à la question suivante.

Question 2. Étant donnés un corps de nombres K et un ensemble infini $\mathcal{E}$ de courbes elliptiques définies sur K, peut-on trouver une constante uniforme $\alpha(\mathcal{E},K)$ telle que pour toute courbe elliptique E appartenant à $\mathcal{E}$, la représentation ρ_p soit irréductible dès que $p > \alpha(\mathcal{E},K)$?

Bien entendu, la réponse à cette question n'est pas toujours positive. Cela s'explique par la présence éventuelle des courbes elliptiques à multiplications complexes. Cependant, dans le cas où $K=\mathbf{Q}$ et $\mathcal{E}$ est l'ensemble de toutes les courbes elliptiques définies sur $\mathbf{Q}$, Mazur a montré ([Maz78]) que tel est le cas avec $\alpha(\mathcal{E},\mathbf{Q}) = 163$. Momose ([Mom95]) a étendu ce résultat avec une constante non effective à tous les corps quadratiques qui ne sont pas des corps quadratiques imaginaires de nombre de classes 1. Dans le cas où $\mathcal{E}$ est l'ensemble des courbes semi-stables, Kraus a également obtenu des résultats uniformes et effectifs pour différents corps de nombres, par exemple les corps de degré 2, 3, 5, 7 ou sur ceux de degré n sur $\mathbf{Q}$ dont la clôture galoisienne a un groupe de Galois sur $\mathbf{Q}$ isomorphe au groupe symétrique $\mathcal{S}_n$ ([Kra96, Kra07]). Dans ce travail, on généralise aux corps de nombres plusieurs critères connus pour $\mathbf{Q}$ (propositions 4.5 et 4.6). On obtient ainsi quelques résultats dans la direction de la question 2 pour des ensembles $\mathcal{E}$ de courbes elliptiques ayant mauvaise réduction additive en une place finie de K et un « défaut de semi-stabilité » particulier. Ces résultats sont particulièrement utiles d'un point de vue numérique et sont illustrés au §4.6.

4.1 Énoncés des résultats

4.1.1 Notations

On note $M_{\mathbf{Z}}$ le sous-ensemble de $\mathbf{Z}[X]$ constitué des polynômes unitaires ne s'annulant pas en 0. L'application

$$\begin{array}{ccc} M_{\mathbf{Z}} \times M_{\mathbf{Z}} & \longrightarrow & \mathbf{Z}[X] \\ (P,Q) & \longmapsto & (P*Q)(X) = \mathrm{Res}_Z\left(P(Z), Q\left(X/Z\right) Z^{\deg Q}\right) \end{array}$$

où Res_Z désigne le résultant par rapport à la variable Z, définit une loi de monoïde commutatif sur $M_{\mathbf{Z}}$ d'élément neutre $X-1$ (lemme 4.22). De plus, les racines complexes de $P*Q$ sont exactement les produits d'une racine de P et d'une racine de Q comptées avec multiplicités (*loc. cit.*).

Soient $P \in M_{\mathbf{Z}}$ et $r \geq 1$. Il existe alors un unique polynôme $P^{(r)} \in M_{\mathbf{Z}}$ tel que

$$P^{(r)}(X^r) = (-1)^{(r+1)\deg P} \prod_{k=0}^{r-1} P(\zeta_r^k X),$$

où ζ_r est une racine r-ième de l'unité dans $\mathbf{C}$ (lemme 4.23). De plus, les racines complexes de $P^{(r)}$ sont exactement les puissances r-ièmes des racines complexes de P comptées avec multiplicités et l'application $P \mapsto P^{(r)}$ est un morphisme de monoïdes pour la loi $*$ (*loc. cit.*).

4.1.2 Résultats

Soient K un corps de nombres contenu dans $\overline{\mathbf{Q}}$ et E une courbe elliptique définie sur K. On note d le degré de K sur $\mathbf{Q}$, D_K son discriminant et $\mathcal{O}_K$ son anneau d'entiers.

Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ en lequel E a bonne réduction. On pose

$$P_{\mathfrak{q}}(X) = X^2 - t_{\mathfrak{q}} X + N(\mathfrak{q}) \in \mathbf{Z}[X]$$

où $N(\mathfrak{q})$ est le cardinal du corps résiduel $\mathcal{O}_K/\mathfrak{q}$ et

$$t_{\mathfrak{q}} = N(\mathfrak{q}) + 1 - A_{\mathfrak{q}},$$

où $A_{\mathfrak{q}}$ est le nombre de points sur le corps résiduel $\mathcal{O}_K/\mathfrak{q}$ de la réduction de E en $\mathfrak{q}$.

Soit ℓ un nombre premier et

$$\ell\mathcal{O}_K = \prod_{\mathfrak{q}|\ell} \mathfrak{q}^{v_{\mathfrak{q}}(\ell)}$$

la décomposition de $\ell\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$. On suppose que E a bonne réduction en chaque idéal premier au-dessus de ℓ. Dans ce cas, on définit le polynôme de P_ℓ^* de $\mathbf{Z}[X]$ par la formule

$$P_\ell^* = \mathop{*}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))}. \tag{4.1}$$

Le polynôme P_ℓ^* ne dépend que de la famille de triplets d'entiers $\{(t_{\mathfrak{q}}, v_{\mathfrak{q}}(\ell), f_{\mathfrak{q}})\}_{\mathfrak{q}|\ell}$ où $N(\mathfrak{q}) = \ell^{f_{\mathfrak{q}}}$ et ses racines complexes sont de module ℓ^{6d} (lemme 4.25). On considère l'entier :

$$B_\ell^{(d)} = \prod_{k=0}^{\left[\frac{d}{2}\right]} P_\ell^*\left(\ell^{12k}\right)$$

où $[d/2]$ désigne la partie entière de $d/2$.

Dans la direction de la question 1 de l'*Introduction*, on montre le critère suivant qui est le résultat principal de ce travail.

Théorème 4.1 *Soit p un nombre premier exceptionnel pour E. Alors, on est dans l'une des situations suivantes :*

1. *p divise $6D_K$;*

2. *il existe un idéal premier* $\mathfrak{p}$ *de* $\mathcal{O}_K$ *divisant* p *en lequel* E *a mauvaise réduction additive avec potentiellement bonne réduction supersingulière.*
3. *pour tout nombre premier* ℓ *tel que* E *a bonne réduction en chaque idéal premier de* $\mathcal{O}_K$ *au-dessus de* ℓ*, le nombre premier* p *divise l'entier* $B_\ell^{(d)}$ *(si* $d = 1$*, on suppose* $\ell \neq p$*).*

Supposons que E soit donnée par une équation de Weierstrass à coefficients dans l'anneau $\mathcal{O}_K$ de discriminant Δ_E et notons $N_{K/\mathbf{Q}}$ la norme de l'extension $K/\mathbf{Q}$. On déduit du théorème 4.1 le corollaire suivant.

Corollaire 4.2 *Soit* p *un nombre premier exceptionnel pour* E*. Alors, on est dans l'une des situations suivantes :*

1. p *divise* $6D_K N_{K/\mathbf{Q}}(\Delta_E)$ *;*
2. *pour tout nombre premier* ℓ *tel que* E *a bonne réduction en chaque idéal premier de* $\mathcal{O}_K$ *au-dessus de* ℓ*, le nombre premier* p *divise l'entier* $B_\ell^{(d)}$ *(si* $d = 1$*, on suppose* $\ell \neq p$*).*

Les racines complexes de P_ℓ^* étant de module ℓ^{6d}, on a en particulier :

$$d \text{ impair } \implies B_\ell^{(d)} \neq 0.$$

On déduit alors du théorème 4.1 le corollaire suivant.

Corollaire 4.3 (cas du degré impair) *On suppose que l'extension* $K/\mathbf{Q}$ *est de degré* d impair*. Alors, l'ensemble des nombres premiers exceptionnels pour* E *est* fini *et inclus dans l'ensemble des diviseurs premiers de l'entier* non nul

$$6D_K N_{K/\mathbf{Q}}(\Delta_E) B_\ell^{(d)},$$

pour tout nombre premier ℓ *tel que* E *a bonne réduction en chaque idéal premier de* $\mathcal{O}_K$ *au-dessus de* ℓ*.*

Remarque. Plus généralement, peut-on caractériser l'ensemble des corps de nombres K possédant la propriété suivante ?

« Pour toute courbe elliptique E définie sur K, l'ensemble $\mathrm{Exc}(E)$ est fini. » D'après [Dav08, th. I], tel est le cas si K ne contient pas le corps de classes de Hilbert d'un corps quadratique imaginaire.

La situation est plus compliquée dans le cas des extensions de degré pair. Cela s'explique *a priori* par la présence de courbes à multiplications complexes avec une infinité de premiers exceptionnels.

Dans le cas particulier des corps quadratiques ($d = 2$), on a une description plus explicite des polynômes P_ℓ^*. On rappelle que pour tout entier $n \geq 1$, il existe un unique polynôme T_n appartenant à $\mathbf{Z}[X]$ tel que pour tout nombre réel θ, on ait

$$T_n(\cos\theta) = \cos(n\theta).$$

Le polynôme T_n s'appelle le n-ième polynôme de Tchebychev (de première espèce). On a en particulier,

$$T_{12}(X) = 2048X^{12} - 6144X^{10} + 6912X^8 - 3584X^6 + 840X^4 - 72X^2 + 1$$

et $T_{24}(X) = 2T_{12}(X)^2 - 1$.

Proposition 4.4 *Soit ℓ nombre premier tel que E a bonne réduction en chaque idéal premier de $\mathcal{O}_K$ divisant ℓ. On est dans l'une des situations suivantes.*

1. *Soit ℓ est ramifié dans K, $\ell\mathcal{O}_K = \mathfrak{q}^2$ et on a*

$$P_\ell^*(X) = P_{\mathfrak{q}}^{(24)}(X) = (X - \ell^{12})^2 + 2\ell^{12}\left(1 - T_{24}\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right)\right)X.$$

En particulier, on a

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_{\mathfrak{q}}^2(t_{\mathfrak{q}}^2 - \ell)^2(t_{\mathfrak{q}}^2 - 4\ell)(t_{\mathfrak{q}}^2 - 2\ell)^2(t_{\mathfrak{q}}^2 - 3\ell)^2(t_{\mathfrak{q}}^4 - 4\ell t_{\mathfrak{q}}^2 + \ell^2)^2.$$

Ainsi $P_\ell^*(\ell^{12}) = 0$ si et seulement si $t_{\mathfrak{q}} \equiv 0 \pmod{\ell}$ (c'est-à-dire pour $\ell \geq 5$, si et seulement si $t_{\mathfrak{q}} = 0$).

2. *Soit ℓ est inerte dans K, $\ell\mathcal{O}_K = \mathfrak{q}$ et on a*

$$P_\ell^*(X) = P_{\mathfrak{q}}^{(12)}(X) = (X - \ell^{12})^2 + 2\ell^{12}\left(1 - T_{12}\left(\frac{t_{\mathfrak{q}}}{2\ell}\right)\right)X.$$

En particulier, on a

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_{\mathfrak{q}}^2(t_{\mathfrak{q}}^2 - \ell^2)^2(t_{\mathfrak{q}}^2 - 4\ell^2)(t_{\mathfrak{q}}^2 - 3\ell^2)^2.$$

Ainsi $P_\ell^*(\ell^{12}) = 0$ si et seulement si $t_{\mathfrak{q}} \equiv 0 \pmod{\ell}$, c'est-à-dire si et seulement si $t_{\mathfrak{q}} = 0$, $\pm\ell$ ou $\pm 2\ell$.

3. *Soit ℓ est décomposé dans K, $\ell\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ et on a*

$$\begin{aligned} P_\ell^*(X) &= (P_{\mathfrak{q}_1} * P_{\mathfrak{q}_2})^{(12)}(X) \\ &= (X^2 - \ell^{24})^2 - 4\ell^{12}\left(T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)X^2 - \ell^{12}\left(T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)^2\right.\right. \\ &\quad \left.\left. + T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)^2\right)X + \ell^{24}T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)\right)X. \end{aligned}$$

En particulier, on a

$$\begin{aligned} P_\ell^*(\ell^{12}) = \ell^{36}\left(t_{\mathfrak{q}_1}^2 - t_{\mathfrak{q}_2}^2\right)^2\left((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 3\ell)^2 - t_{\mathfrak{q}_1}^2t_{\mathfrak{q}_2}^2\right)^2\left(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 4\ell\right)^2 \\ \times\left((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - \ell)^2 - 3t_{\mathfrak{q}_1}^2t_{\mathfrak{q}_2}^2\right)^2. \end{aligned}$$

Ainsi $P_\ell^*(\ell^{12}) = 0$ si et seulement si l'une des conditions suivantes est satisfaite :

$$t_{\mathfrak{q}_1} = \pm t_{\mathfrak{q}_2}; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 \pm t_{\mathfrak{q}_1}t_{\mathfrak{q}_2} = 3\ell; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 = 4\ell.$$

Remarques/questions.

1. Dans le cas où $d = 1$ (*i.e.* $K = \mathbf{Q}$) et $\ell \geq 5$, on a $P_\ell^*(\ell^6) \neq 0$ si et seulement si E a bonne réduction ordinaire en ℓ. Or on sait que l'ensemble des nombres premiers supersinguliers a pour densité 0 dans l'ensemble des nombres premiers si E est sans multiplication complexe et $1/2$ sinon. Il existe donc une infinité de nombres premiers ℓ tels que $P_\ell^*(\ell^6) \neq 0$.

2. Dans le cas où $d = 2$, on a

$$B_\ell^{(2)} = P_\ell^*(1) \cdot P_\ell^*(\ell^{12}) \quad \text{et} \quad P_\ell^*(1) \neq 0.$$

Pour autant, on ne sait pas caractériser l'ensemble des courbes elliptiques pour lesquelles il existe un nombre premier ℓ tel que $B_\ell^{(2)}$ soit non nul. Par exemple, est-ce toujours le cas si E est sans multiplication complexe ? D'après la proposition 4.4, cela résulterait en particulier de l'énoncé suivant : il existe un idéal premier de *degré* 2 en lequel E a bonne réduction *ordinaire*.

3. Toujours dans le cas $d = 2$, si E n'est pas une $\mathbf{Q}$-courbe (*i.e.* E n'est pas isogène à sa conjuguée galoisienne), on montre en utilisant [Ser72, th.6] et [Fal86] qu'il existe un nombre premier ℓ décomposé dans K ($\ell\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$) tel que $t_{\mathfrak{q}_1} \neq \pm t_{\mathfrak{q}_2}$. Cela ne suffit pas à assurer le fait que $B_\ell^{(2)}$ soit non nul.

4. Plus généralement, si $d \geq 2$ et E est sans multiplication complexe, existe-t-il un nombre premier ℓ tel que $P_\ell^*(\ell^{6d}) \neq 0$?

Dans la direction de la question 2 de l'*Introduction*, on généralise aux corps de nombres plusieurs résultats connus sur $\mathbf{Q}$. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ de caractéristique résiduelle ℓ. On a

$$N(\mathfrak{q}) = |\mathcal{O}_K/\mathfrak{q}| = \ell^{f_\mathfrak{q}},$$

où $f_\mathfrak{q}$ est le degré résiduel de $\mathfrak{q}$. On suppose que E a mauvaise réduction additive en $\mathfrak{q}$ avec potentiellement bonne réduction. Alors, pour tout nombre premier $p \geq 3$ tel que $p \neq \ell$, l'action de $I_\mathfrak{q}$, sous-groupe d'inertie en $\mathfrak{q}$, sur $E[p]$ se fait par l'intermédiaire d'un certain quotient fini $\Phi_\mathfrak{q}$ de $I_\mathfrak{q}$ ([ST68]) :

$$I_\mathfrak{q} \longrightarrow \Phi_\mathfrak{q} \hookrightarrow \mathrm{Aut}(E[p]).$$

On a alors les deux résultats suivants. Ceux-ci sont connus pour $K = \mathbf{Q}$ et ont été utilisés par Serre dans [Ser72, §5] pour traiter des exemples numériques.

Proposition 4.5 *On suppose que le groupe $\Phi_\mathfrak{q}$ n'est pas cyclique. Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$.*

Proposition 4.6 *On suppose que pour tout entier $n \geq 0$, l'ordre du groupe $\Phi_\mathfrak{q}$ ne divise pas $N(\mathfrak{q})^n(N(\mathfrak{q}) - 1)$. Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 3$ tel que $p \neq \ell$.*

Remarque. Si $\ell \geq 5$, on peut remplacer l'hypothèse par : l'ordre du groupe $\Phi_\mathfrak{q}$ ne divise pas $N(\mathfrak{q}) - 1$.

Comme corollaires des propositions ci-dessus, on obtient les résultats suivants dans le cas où $\mathfrak{q}$ divise 2 ou 3.

Corollaire 4.7 *On suppose que $\mathfrak{q}$ divise 2 et que l'une des conditions suivantes est satisfaite :*

1. *le groupe $\Phi_\mathfrak{q}$ est d'ordre 8 ou 24 ;*
2. *le groupe $\Phi_\mathfrak{q}$ est d'ordre 3 ou 6 et le degré résiduel $f_\mathfrak{q}$ est impair.*

Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$.

Lorsque $\mathfrak{q}$ divise 2, l'étude faite au Chapitre 3 permet parfois de calculer l'ordre du groupe $\Phi_\mathfrak{q}$ directement à partir de la valuation de l'invariant modulaire de E (théorème 3.1). Si K est une extension quadratique de $\mathbf{Q}$ (ou plus généralement si le degré sur $\mathbf{Q}_2$ du complété de K en $\mathfrak{q}$ est ≤ 2), le théorème 3.2 avec le théorème 3.84 et [Cal04] fournissent en toute généralité l'ordre du groupe $\Phi_\mathfrak{q}$ en fonction des coefficients d'une équation de Weierstrass de E.

Remarque. La condition de parité dans le corollaire précédent est nécessaire. En effet, soient K l'extension de $\mathbf{Q}$ engendrée par une racine du polynôme

$$(X^2+5X+1)^3(X^2+13X+49) - \frac{2^4 \cdot 13^3}{3^2}X$$

et E la courbe elliptique définie sur K par l'équation

$$y^2 = x^3 - x^2 - 4x - 4.$$

Alors, le degré résiduel de K en l'unique idéal $\mathfrak{p}_2$ de $\mathcal{O}_K$ divisant 2, est $f_{\mathfrak{p}_2} = 2$ et la courbe E a un défaut de semi-stabilité d'ordre 6 en $\mathfrak{p}_2$. Pour autant la représentation $\rho_7 : \mathrm{G}_K \longrightarrow \mathrm{GL}_2(\mathbf{F}_7)$ est *réductible* car K correspond au sous-corps de $\overline{\mathbf{Q}}$ laissé fixe par le stablilisateur dans $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ d'un sous-groupe d'ordre 7 de $E(\overline{\mathbf{Q}})$ ([KO92, p.273]).

Lorsque $\mathfrak{q}$ divise 3, on a le corollaire suivant.

Corollaire 4.8 *On suppose que $\mathfrak{q}$ divise 3 et que l'une des conditions suivantes est satisfaite :*

1. *le groupe $\Phi_\mathfrak{q}$ est d'ordre 12 ;*
2. *le groupe $\Phi_\mathfrak{q}$ est d'ordre 4 et le degré résiduel $f_\mathfrak{q}$ est impair.*

Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$.

4.2 Rappels

Dans toute cette section, on fixe un corps de nombres K contenu dans $\overline{\mathbf{Q}}$ et une courbe elliptique E définie sur K. Soit p un nombre premier exceptionnel. Le groupe $E[p]$ possède alors une droite D stable par G_K. Notons λ le caractère donnant l'action de G_K sur D. On l'appelle caractère d'isogénie associé à D. Dans une base convenable de $E[p]$ sur $\mathbf{F}_p$, la représentation ρ_p est représentable matriciellement par

$$\begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

où λ et λ' s'interprètent comme des caractères de G_K à valeurs dans $\mathbf{F}_p^*$. On a

$$\det \rho_p = \lambda \cdot \lambda' = \chi_p, \tag{4.2}$$

où χ_p est le caractère donnant l'action de G_K sur les racines p-ièmes de l'unité (caractère cyclotomique).

La représentation ρ_p se factorise à travers le groupe de Galois de l'extension $K(E[p])/K$, où $K(E[p])$ est le corps engendré sur K par les coordonnées des

points de p-torsion de E. On note encore ρ_p, λ, λ' et χ_p les morphismes passés au quotient.

Soit $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_K$. On note $I_\mathfrak{q}$ un sous-groupe d'inertie en $\mathfrak{q}$ de $\mathrm{Gal}(K(E[p])/K)$. Si E a bonne réduction en $\mathfrak{q}$ et $\mathfrak{q}$ ne divise pas p, l'extension $K(E[p])/K$ est non ramifiée en $\mathfrak{q}$ par le critère de Néron-Ogg-Shafarevich. On note $\sigma_\mathfrak{q}$ une subsitution de Frobenius en $\mathfrak{q}$ de $\mathrm{Gal}(K(E[p])/K)$ (bien définie à conjugaison près).

Le résultat suivant est bien connu (*c.f.* [Sil92, Th.2.4]).

Proposition 4.9 (Hasse – Weil) *Soit $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_K$ en lequel E a bonne réduction. Les racines complexes de $P_\mathfrak{q}$ sont de module $N(\mathfrak{q})^{1/2}$. En particulier, on a*

$$|t_\mathfrak{q}| \leq 2N(\mathfrak{q})^{1/2}.$$

Si de plus $\mathfrak{q}$ ne divise pas p, le polynôme caractéristique de $\rho_p(\sigma_\mathfrak{q})$ est $\overline{P_\mathfrak{q}} = P_\mathfrak{q} \pmod p \in \mathbf{F}_p[X]$. En particulier, on a

$$\overline{P_\mathfrak{q}}(\lambda(\sigma_\mathfrak{q})) = 0.$$

4.2.1 Courbes sans multiplication complexe

Dans ce § on démontre la finitude de l'ensemble des nombres premiers exceptionnels dans le cas des courbes sans multiplication complexe à partir du corollaire suivant du théorème de Shafarevich (lui-même conséquence du théorème de Siegel).

Proposition 4.10 (Shafarevich) *Il n'existe qu'un nombre fini (à K-isomorphisme près) de courbes elliptiques E' définies sur K et isogènes à E sur K.*

On a le résultat suivant ([Sil92, cor. 6.3]).

Proposition 4.11 (Serre) *On suppose que la courbe E est sans multiplication complexe. Alors, l'ensemble des nombres premiers exceptionnels pour E est fini.*

Démonstration. Soit p un nombre premier exceptionnel. Il existe alors un sous-groupe cyclique stable d'ordre p, noté D_p, une courbe elliptique notée E_p définie sur K et une isogénie définie sur K

$$\phi_p \ : E \longrightarrow E_p$$

telle que $\ker \phi_p = D_p$. Supposons que l'ensemble des nombres premiers exceptionnels de E soit infini. D'après la proposition précédente, il existe alors une infinité de nombres premiers p tels que les courbes E_p correspondantes appartiennent à la même classe d'isomorphisme. Soient p et p' deux nombres premiers exceptionnels tels que $E_p \simeq E_{p'}$. La composition

$$E \xrightarrow{\phi_p} E_p \simeq E_{p'} \xrightarrow{\hat{\phi}_{p'}} E,$$

où $\hat{\phi}_{p'}$ est l'isogénie duale de $\phi_{p'}$ fournit un endomorphisme de E de degré

$$(\deg \phi_p)(\deg \hat{\phi}_{p'}) = p \cdot p'.$$

Or, par hypothèse, $\mathrm{End}(E) = \mathbf{Z}$, donc chaque endomorphisme de E est de degré n^2 pour un certain entier $n \in \mathbf{Z}$. D'où $p = p'$ et les courbes E_p sont deux-à-deux non isomorphes. On en déduit la finitude de l'ensemble des nombres premiers exceptionnels.

4.2.2 Ramification et caractère d'isogénie

On suppose que p est un nombre premier exceptionnel pour E. L'objectif de ce § est de démontrer le résultat suivant.

Proposition 4.12 *Supposons $p \geq 5$ non ramifié dans K.*

1. *Le caractère λ^{12} est non ramifié en dehors des idéaux premiers de $\mathcal{O}_K$ divisant p.*
2. *Soit $\mathfrak{p}$ un idéal de $\mathcal{O}_K$ divisant p. On suppose que E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2 (supersingulière). Alors, il existe un entier $\alpha_{\mathfrak{p}} \in \{0, 12\}$ tel que*

$$\lambda^{12} |_{I_{\mathfrak{p}}} = \chi_p^{\alpha_{\mathfrak{p}}} |_{I_{\mathfrak{p}}} .$$

Remarque. Dans une base convenable, la représentation sur les points de p-torsion de la courbe E/D est représentable matriciellement par

$$\begin{pmatrix} \lambda' & * \\ 0 & \lambda \end{pmatrix}.$$

Autrement dit, d'après l'égalité (4.2), on peut toujours, si on le souhaite, remplacer la famille $\{\alpha_{\mathfrak{p}}\}_{\mathfrak{p}|p}$ par la famille $\{12 - \alpha_{\mathfrak{p}}\}_{\mathfrak{p}|p}$.

La proposition 4.12 se déduit de l'étude locale, donnée aux §§4.2.2–4.2.2, de la restriction de ρ_p aux sous-groupes d'inertie de $\mathrm{Gal}(K(E[p])/K)$. Ces résultats étant connus, nous les admettrons tout en donnant les références où trouver les détails (voir aussi [Dav08, §1] pour une discussion similaire).

Notations. On note j l'invariant modulaire de E, S_E l'ensemble des idéaux premiers de $\mathcal{O}_K$ en lesquels E a mauvaise réduction et S'_E le sous-ensemble de S_E constitué des idéaux premiers de mauvaise réduction additive. Pour un idéal premier $\mathfrak{q}$ de $\mathcal{O}_K$, on note $v_{\mathfrak{q}}$ la valuation en $\mathfrak{q}$ de K normalisée par $v_{\mathfrak{q}}(K^*) = \mathbf{Z}$.

Étude de la représentation ρ_p hors de p

Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ ne divisant pas p. Le résultat suivant résulte du critère de Néron-Ogg-Shafarevich ([Sil92, p.184]).

Proposition 4.13 *Si $\mathfrak{q}$ n'appartient pas à S_E, alors E a bonne réduction en $\mathfrak{q}$ et $I_{\mathfrak{q}}$ agit trivialement sur $E[p]$.*

Le résultat suivant est une conséquence de la théorie de la courbe de Tate (*c.f.* [Ser68, IV]).

Proposition 4.14 *Supposons que $\mathfrak{q}$ appartienne à S_E et $v_{\mathfrak{q}}(j) < 0$. Alors :*

1. *soit E a mauvaise réduction multiplicative en $\mathfrak{q}$ et on a*

$$\rho_p |_{I_{\mathfrak{q}}} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

où $I_{\mathfrak{q}}$ agit trivialement si et seulement si $v_{\mathfrak{q}}(j) \equiv 0 \pmod{p}$.

2. *Soit E a mauvaise réduction additive en $\mathfrak{q}$ (avec potentiellement réduction multiplicative) et on a*

$$\rho_p \mid_{I_\mathfrak{q}} \simeq \begin{pmatrix} \varepsilon & * \\ 0 & \varepsilon \end{pmatrix},$$

où $\varepsilon : I_\mathfrak{q} \to \{\pm 1\}$ est un caractère quadratique.

Le résultat suivant utilise l'hypothèse $p \geq 5$.

Proposition 4.15 *Si $\mathfrak{q}$ appartient à S'_E et $v_\mathfrak{q}(j) \geq 0$, alors l'image de $I_\mathfrak{q}$ par λ dans $\mathbf{F}_p^*$ est isomorphe au groupe $\Phi_\mathfrak{q}$; c'est un sous-groupe cyclique d'ordre 2, 3, 4 ou 6.*

Étude de la représentation ρ_p en p

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ divisant p. On rappelle que p est ≥ 5 et non ramifié dans K. On note $\Delta_\mathfrak{p}$ le discriminant d'une équation de Weierstrass de E minimale en $\mathfrak{p}$.

Le résultat suivant se trouve dans [Ser72, §§1.11-1.12].

Proposition 4.16 *Si $\mathfrak{p}$ n'appartient pas à S'_E, alors E a soit mauvaise réduction multiplicative, soit bonne réduction ordinaire en $\mathfrak{p}$ et on a*

$$\rho_p \mid_{I_\mathfrak{p}} \simeq \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}.$$

Le résultat suivant est l'énoncé de la prop. 10 de [Kra97a].

Proposition 4.17 *Si $\mathfrak{p}$ appartient à S'_E et $v_\mathfrak{p}(j) < 0$, alors, on a*

$$\rho_p \mid_{I_\mathfrak{p}} \simeq \begin{pmatrix} \chi_p^{p-\alpha} & * \\ 0 & \chi_p^{\alpha} \end{pmatrix}, \quad \text{où } \alpha = \frac{p-1}{2}.$$

Le résultat suivant résulte de [Kra97a, prop.1] et [Kra97a, lem.2].

Proposition 4.18 *Si $\mathfrak{p}$ appartient à S'_E, $v_\mathfrak{p}(j) \geq 0$ et E a potentiellement bonne réduction de hauteur $h = 1$. Alors, le nombre $\alpha = (p-1)v_\mathfrak{p}(\Delta_\mathfrak{p})/12$ est entier et on a*

$$\rho_p \mid_{I_\mathfrak{p}} \simeq \begin{pmatrix} \chi_p^{1-\alpha} & * \\ 0 & \chi_p^{\alpha} \end{pmatrix}.$$

Démonstration de la proposition 4.12

On aura besoin du lemme suivant.

Lemme 4.19 *Soit H un sous-groupe de $\mathrm{Gal}(K(E[p])/K)$. On suppose que dans deux bases de $E[p]$ sur $\mathbf{F}_p$, la restriction de ρ_p à H est représentable matriciellement par*

$$\begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \mu & * \\ 0 & \mu' \end{pmatrix}.$$

Alors, on a $\{\lambda, \lambda'\} = \{\mu, \mu'\}$ (où l'on note encore λ et λ' les restrictions des caractères à H et où μ, μ' sont des caractères de H à valeurs dans $\mathbf{F}_p$).

Démonstration. Notons (P_1, P_2) et (P_3, P_4) les deux bases de $E[p]$ sur $\mathbf{F}_p$ où $\rho_p \mid_H$ est représentable respectivement par les matrices $\begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}$ et $\begin{pmatrix} \mu & * \\ 0 & \mu' \end{pmatrix}$. Pour $1 \leq i \leq 4$, notons D_i la droite engendrée par P_i. Si $D_1 \neq D_3$, alors dans la base (P_1, P_3), $\rho_p \mid_H$ est représentable matriciellement sous la forme

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}.$$

On a alors $\lambda = \mu'$ car pour tout σ dans H, les valeurs propres de $\rho_p(\sigma)$ sont $\mu(\sigma)$ et $\mu'(\sigma)$. D'où $\lambda' = \mu$. Si $D_1 = D_3$, alors H agit sur une même droite par les caractères λ et μ. Donc, $\lambda = \mu$ et par suite, $\lambda' = \mu'$. D'où le lemme 4.19.

Démontrons à présent la proposition 4.12. On distingue deux cas.

1. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ ne divisant pas p. D'après l'étude locale du §4.2.2, on est dans l'une des situations suivantes.
   (a) La courbe E a bonne réduction en $\mathfrak{q}$ et d'après la proposition 4.13, $E[p]$ est non ramifié en $\mathfrak{q}$, donc λ également et par conséquent sa puissance 12-ième.
   (b) La courbe E a potentiellement réduction multiplicative (y compris réduction multiplicative) en $\mathfrak{q}$ et d'après la proposition 4.14 et le lemme 4.19, on a
   $$\lambda^2 \mid_{I_\mathfrak{q}} = 1.$$
   En particulier, λ^{12} est non ramifié en $\mathfrak{q}$.
   (c) La courbe E a mauvaise réduction additive en $\mathfrak{q}$ et d'après la proposition 4.15, on a
   $$\lambda^n \mid_{I_\mathfrak{q}} = 1, \quad \text{avec } n = 2, 3, 4 \text{ ou } 6.$$
   En particulier, λ^{12} est non ramifié en $\mathfrak{q}$.

   Cela démontre le premier point de la proposition 4.12.
2. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ divisant p. D'après l'étude locale du §4.2.2 et les hypothèses de l'énoncé, on est dans l'une des situations suivantes.
   (a) La courbe E a soit mauvaise réduction multiplicative, soit bonne réduction ordinaire en $\mathfrak{p}$ et d'après la proposition 4.16 et le lemme 4.19 on a
   $$\lambda \mid_{I_\mathfrak{p}} = \chi_p \mid_{I_\mathfrak{p}} \quad \text{ou} \quad \lambda \mid_{I_\mathfrak{p}} = 1.$$
   D'où
   $$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} \quad \text{avec } \alpha_\mathfrak{p} = 0 \text{ ou } 12.$$
   (b) La courbe E a mauvaise réduction additive avec potentiellement réduction multiplicative en $\mathfrak{p}$ et d'après la proposition 4.17 et le lemme 4.19 on a
   $$\lambda^{12} \mid_{I_\mathfrak{p}} = \left(\chi_p \mid_{I_\mathfrak{p}}\right)^{12-12\alpha} \quad \text{ou} \quad \lambda^{12} \mid_{I_\mathfrak{p}} = \left(\chi_p \mid_{I_\mathfrak{p}}\right)^{12\alpha}, \quad \text{où } \alpha = \frac{p-1}{2}.$$
   Or, $\chi_p \mid_{I_\mathfrak{p}}$ est d'ordre $p-1$ et $12\alpha \equiv 0 \pmod{(p-1)}$. Donc, on a
   $$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} \quad \text{avec } \alpha_\mathfrak{p} = 0 \text{ ou } 12.$$

(c) La courbe E a mauvaise réduction additive avec potentiellement bonne réduction de hauteur $h = 1$ en $\mathfrak{p}$. D'après la proposition 4.18 et le lemme 4.19 on a alors $h = 1$ et

$$\lambda^{12} \mid_{I_\mathfrak{p}} = \left(\chi_p \mid_{I_\mathfrak{p}}\right)^{12-12\alpha} \quad \text{ou} \quad \lambda^{12} \mid_{I_\mathfrak{p}} = \left(\chi_p \mid_{I_\mathfrak{p}}\right)^{12\alpha},$$

où $\alpha = (p-1)v_\mathfrak{p}(\Delta_\mathfrak{p})/12$. Or, $\chi_p \mid_{I_\mathfrak{p}}$ est d'ordre $p-1$ et $12\alpha \equiv 0 \pmod{(p-1)}$. Donc, on a

$$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} \quad \text{avec } \alpha_\mathfrak{p} = 0 \text{ ou } 12.$$

Cela achève la démonstration de la proposition 4.12.

Remarques.

1. On peut montrer en utilisant la description locale de ρ_p donnée dans la proposition [Kra97a, prop.2] que si $\mathfrak{p}$ divise p et E a mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction supersingulière, alors il existe un entier $\alpha_\mathfrak{p} \in \{4, 6, 8\}$ tel que

$$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} .$$

2. Dans sa thèse ([Dav08]), A. David démontre que si K ne contient pas le corps de classes de Hilbert d'un corps quadratique imaginaire, il existe alors une constante effective $C(K)$, ne dépendant que de K (et donc pas de E) telle que si $p > C(K)$, on a $\alpha_\mathfrak{p} = 6$ pour *tout* idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p (voir également [Mom95]). Nous n'utiliserons pas ces résultats.

4.2.3 Théorie du corps de classes et caractère d'isogénie

On reprend les hypothèses et notations précédentes. En particulier, p est un nombre premier ≥ 5 non ramifié dans K et on suppose que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p, E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2. Étant donné un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus de p, on désigne par

$$N_\mathfrak{p} : (\mathcal{O}_K/\mathfrak{p})^* \longrightarrow \mathbf{F}_p^*$$

le morphisme norme. L'objectif de ce § est de démontrer la proposition ci-dessous. Elle figure déjà sous une forme légèrement différente dans la thèse de David ([Dav08, prop.2.2.1]).

Proposition 4.20 (David) *Soit ℓ un nombre premier $\neq p$ et $\ell\mathcal{O}_K = \prod_{\mathfrak{q}|\ell} \mathfrak{q}^{v_\mathfrak{q}(\ell)}$ la décomposition de $\ell\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$. On suppose que pour tout idéal premier $\mathfrak{q}$ de $\mathcal{O}_K$ divisant ℓ, E a bonne réduction en $\mathfrak{q}$. Alors, on a :*

$$\prod_{\mathfrak{q}|\ell} \lambda(\sigma_\mathfrak{q})^{12v_\mathfrak{q}(\ell)} = \prod_{\mathfrak{p}|p} N_\mathfrak{p}(\ell + \mathfrak{p})^{\alpha_\mathfrak{p}},$$

où $\alpha_\mathfrak{p} \in \{0, 12\}$ est défini à la proposition 4.12.

Un lemme de la théorie du corps de classes

Soient L l'extension de K trivialisant le caractère λ^{12} et μ_p le groupe de racines p-ièmes de l'unité dans $\overline{\mathbf{Q}}$. D'après l'accouplement de Weil, on a $\mu_p \subset K(E[p])$. Donc $L(\mu_p)$ est une sous-extension abélienne de $K(E[p])/K$. On note I_K le groupe des idèles de K et

$$r \ : I_K \longrightarrow \mathrm{Gal}(L(\mu_p)/K),$$

le morphisme de réciprocité global donné par la théorie du corps de classes. Il est surjectif et son noyau contient les idèles principales.

Soit v une place de K. On note K_v le complété de K en v et on identifie K à un sous-corps de K_v. On désigne par

$$r_v \ : K_v^* \hookrightarrow I_K \longrightarrow \mathrm{Gal}(L(\mu_p)/K)$$

la composée de l'injection de K_v^* dans I_K par le morphisme de réciprocité global.

Si $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_K$ de bonne réduction ne divisant pas p, on rappelle que l'extension $K(E[p])/K$ est non ramifiée en $\mathfrak{q}$. La restriction à $\mathrm{Gal}(L(\mu_p)/K)$ d'une substitution de Frobenius en $\mathfrak{q}$ du groupe $\mathrm{Gal}(K(E[p])/K)$ (bien définie à conjugaison près) est unique. On la note encore $\sigma_\mathfrak{q}$. De même, on note encore χ_p (resp. λ) la restriction du caractère cyclotomique (resp. d'isogénie) à $\mathrm{Gal}(L(\mu_p)/K)$.

Le résultat suivant regroupe plusieurs résultats classiques de la théorie du corps de classes qui seront utiles à la démonstration de la proposition 4.20. La démonstration du troisième point est tirée de [Kra07, App. 1 prop. 1].

Lemme 4.21 *Soit v une place de K.*

1. *Si v est une place infinie de K, on a $\lambda^{12}(r_v(\ell)) = 1$.*
2. *Si $v = \mathfrak{q}$ est une place finie de K ne divisant pas p, on a*

$$r_\mathfrak{q}(\mathcal{U}_\mathfrak{q}) = \{1\},$$

où $\mathcal{U}_\mathfrak{q}$ est le groupe des unités de l'anneau d'entiers du corps $K_\mathfrak{q}$. Si de plus, $\mathfrak{q}$ divise ℓ, alors

$$r_\mathfrak{q}(\pi_\mathfrak{q}) = \sigma_\mathfrak{q},$$

où $\pi_\mathfrak{q}$ est une uniformisante de $K_\mathfrak{q}$.

3. *Si $v = \mathfrak{p}$ est une place finie de K divisant p, alors $r_\mathfrak{p}(\ell)$ appartient au sous-groupe d'inertie en $\mathfrak{p}$ de $L(\mu_p)/K$ et on a*

$$\chi_p\left(r_\mathfrak{p}(\ell)\right) = N_\mathfrak{p}(\ell + \mathfrak{p})^{-1}.$$

Démonstration. Soit v une place de K. On distingue trois cas.

1. Supposons que v soit une place infinie de K. Soit L' l'extension de K trivialisant le caractère λ,

$$r' \ : I_K \longrightarrow \mathrm{Gal}(L'(\mu_p)/K),$$

le morphisme de réciprocité global donné par la théorie du corps de classes et

$$r'_v \ : K_v^* \hookrightarrow I_K \xrightarrow{r'} \mathrm{Gal}(L'(\mu_p)/K).$$

L'image de l'application r'_v est d'ordre ≤ 2. Par ailleurs, l'image par λ^{12} d'un élément de $\mathrm{Gal}(L'(\mu_p)/K)$ ne dépend que de sa restriction à $\mathrm{Gal}(L(\mu_p)/K)$. D'où :

$$\lambda^{12}(r_v(\ell)) = \lambda^{12}(r'_v(\ell)),$$

puis

$$\lambda(r'_v(\ell))^{12} = \lambda(r'_v(\ell)^{12}) = 1.$$

D'où le résultat.

2. Supposons que $v = \mathfrak{q}$ soit une place finie de K ne divisant pas p. Alors, d'après [Neu86], l'image par $r_\mathfrak{q}$ de $\mathcal{U}_\mathfrak{q}$ est un sous-groupe d'inertie en $\mathfrak{q}$ de l'extension $L(\mu_p)/K$. Or celle-ci est non ramifiée en $\mathfrak{q}$ d'après le lemme 4.19. D'où l'égalité

$$r_\mathfrak{q}(\mathcal{U}_\mathfrak{q}) = \{1\}.$$

Si de plus $\mathfrak{q}$ divise ℓ alors E a bonne réduction en $\mathfrak{q}$ et d'après [Neu86], l'image par $r_\mathfrak{q}$ de $\pi_\mathfrak{q}$ est la substitution de Frobenius en $\mathfrak{q}$ de l'extension $L(\mu_p)/K$. Autrement dit, $r_\mathfrak{q}(\pi_\mathfrak{q}) = \sigma_\mathfrak{q}$.

3. Supposons que $v = \mathfrak{p}$ soit une place finie de K divisant p. On note $\overline{\mathbf{Q}_p}$ une clôture algébrique de $\mathbf{Q}_p$. Comme p est non ramifié dans K, on identifie $K_\mathfrak{p}$ à l'extension non ramifiée de $\mathbf{Q}_p$ contenue dans $\overline{\mathbf{Q}_p}$ dont le degré sur $\mathbf{Q}_p$ est le degré résiduel de $\mathfrak{p}$ sur p. On note K^{ab} la clôture abélienne de K dans $\overline{\mathbf{Q}}$, $K_\mathfrak{p}^{ab}$ la clôture abélienne de $K_\mathfrak{p}$ dans $\overline{\mathbf{Q}_p}$,

$$\Theta_\mathfrak{p} \ : K_\mathfrak{p}^* \longrightarrow \mathrm{Gal}(K_\mathfrak{p}^{ab}/K_\mathfrak{p})$$

le morphisme de réciprocité local en $\mathfrak{p}$ et

$$\mathrm{Res}_\mathfrak{p} \ : \mathrm{Gal}(K_\mathfrak{p}^{ab}/K_\mathfrak{p}) \longrightarrow \mathrm{Gal}(L(\mu_p)/K)$$

le morphisme de restriction. D'après la compatibilité entre la théorie du corps de classes locale et globale, on a, pour tout $x \in K_\mathfrak{p}^*$,

$$\mathrm{Res}_\mathfrak{p}(\Theta_\mathfrak{p}(x)) = r_\mathfrak{p}(x). \tag{4.3}$$

Or, d'après le corollaire de [Kra07, App. 1 prop. 1], on a

$$\Theta_\mathfrak{p}(\ell)(\zeta) = \zeta^{n^{-1}},$$

où n est un entier tel que

$$N_\mathfrak{p}(\ell + \mathfrak{p}) = n \pmod{p\mathbf{Z}}.$$

D'où le résultat voulu, d'après l'égalité (4.3).

Cela termine la démonstration du lemme 4.21.

Démonstration de la proposition 4.20

L'image par le morphisme de réciprocité global de l'idèle principale $(\ell)_v$ est triviale, *i.e.*

$$\prod_v r_v(\ell) = 1. \tag{4.4}$$

Si v est une place infinie de K, alors d'après le lemme 4.21, on a

$$\lambda^{12}\left(r_v(\ell)\right) = 1. \tag{4.5}$$

Si $v = \mathfrak{q}$ est une place finie de K ne divisant ni p, ni ℓ on a $\ell \in \mathcal{U}_{K_\mathfrak{q}}$. D'après *loc. cit.* on a donc $r_\mathfrak{q}(\ell) = 1$.

Si $v = \mathfrak{q}$ est une place finie de K divisant ℓ. Alors,

$$\ell = u \cdot \pi_\mathfrak{q}^{v_\mathfrak{q}(\ell)},$$

où $\pi_\mathfrak{q}$ est une uniformisante de $K_\mathfrak{q}$ et $u \in \mathcal{U}_{K_\mathfrak{q}}$. D'après *loc. cit.* on a donc $r_\mathfrak{q}(\ell) = \sigma_\mathfrak{q}^{v_\mathfrak{q}(\ell)}$, puis

$$\lambda^{12}\left(r_\mathfrak{q}(\ell)\right) = \left(\lambda^{12}(\sigma_\mathfrak{q})\right)^{v_\mathfrak{q}(\ell)} = \lambda(\sigma_\mathfrak{q})^{12 v_\mathfrak{q}(\ell)}. \tag{4.6}$$

Si $v = \mathfrak{p}$ est une place finie de K divisant p, alors d'après *loc. cit.*, $r_\mathfrak{p}(\ell)$ appartient au sous-groupe d'inertie en $\mathfrak{p}$ de $L(\mu_p)/K$ et on a

$$\chi_p\left(r_\mathfrak{p}(\ell)\right) = N_\mathfrak{p}(\ell + \mathfrak{p})^{-1}.$$

Or, d'après la proposition 4.12, on a

$$\lambda^{12}\mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}}\mid_{I_\mathfrak{p}}.$$

On en déduit que l'on a

$$\lambda^{12}\left(r_\mathfrak{p}(\ell)\right) = N_\mathfrak{p}(\ell + \mathfrak{p})^{-\alpha_\mathfrak{p}}. \tag{4.7}$$

D'après les égalités (4.4)–(4.7) ci-dessus, on a

$$\begin{aligned} 1 &= \prod_v \lambda^{12}\left(r_v(\ell)\right) \\ &= \prod_{\mathfrak{q}\mid\ell} \lambda(\sigma_\mathfrak{q})^{12 v_\mathfrak{q}(\ell)} \cdot \prod_{\mathfrak{p}\mid p} N_\mathfrak{p}(\ell + \mathfrak{p})^{-\alpha_\mathfrak{p}}. \end{aligned}$$

Cela démontre la proposition 4.20.

4.3 Démonstration du théorème 4.1

Soient K un corps de nombres contenu dans $\overline{\mathbf{Q}}$, E une courbe elliptique définie sur K et p un nombre premier exceptionnel. On suppose $p \geq 5$, p non ramifié dans K et pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p, E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2.

Soit ℓ un nombre premier tel que E ait bonne réduction en tout idéal premier de $\mathcal{O}_K$ divisant ℓ. Il s'agit de montrer que p divise $B_\ell^{(d)}$.

La démonstration du théorème 4.1 comporte plusieurs étapes. On commence par définir pour tout anneau intègre A une loi de monoïde commutatif sur le sous-ensemble de $A[X]$ constitué des polynômes unitaires ne s'annulant pas en 0 (lemme 4.22). Cela nous permet de démontrer les propriétés suivantes du polynôme P_ℓ^* (lemme 4.25) :

- ses racines complexes sont de module ℓ^{6d} ;
- le membre de gauche de l'égalité de la proposition 4.20 est une racine de $\overline{P_\ell^*} = P_\ell^* \pmod p$.

Le théorème 4.1 se déduit alors d'une reformulation du membre de droite de la proposition 4.20.

4.3.1 Loi de monoïde

Soit A un anneau intègre de corps des fractions L et $\overline{L}$ une clôture algébrique de L. On note M_A le sous-ensemble de $A[X]$ constitué des polynômes unitaires ne s'annulant pas en 0.

Lemme 4.22 *L'application*

$$\begin{array}{ccc} M_A \times M_A & \longrightarrow & A[X] \\ (P,Q) & \longmapsto & (P*Q)(X) = \mathrm{Res}_Z\left(P(Z), Q\left(X/Z\right) Z^{\deg Q}\right) \end{array}$$

a une image contenue dans M_A. Elle définit une loi de monoïde commutatif sur M_A d'élément neutre $P_0(X) = X - 1$. De plus, si P, $Q \in M_A$ s'écrivent

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \quad \textit{et} \quad Q(X) = \prod_{j=1}^{m}(X - \beta_j)$$

dans $\overline{L}[X]$, on a

$$(P*Q)(X) = \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (X - \alpha_i\beta_j).$$

En particulier,

$$(P*Q)(0) = (-1)^{\deg P\cdot\deg Q} P(0)^{\deg Q} Q(0)^{\deg P}.$$

Démonstration. Il s'agit de vérifier que pour tout P, Q et $R \in M_A$, on a

1. $P*Q \in M_A$;
2. $P*P_0 = P_0*P = P$;
3. $(P*Q)*R = P*(Q*R)$;
4. $P*Q = Q*P$.

On suppose que le polynôme Q s'écrit

$$Q(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0, \quad \text{avec } b_0 \neq 0.$$

Alors,

$$Q\left(\frac{X}{Z}\right) Z^m = b_0Z^m + b_1XZ^{m-1} + \cdots + b_{m-1}X^{m-1}Z + X^m \in A[X][Z]$$

et $\deg_Z(Q(X/Z)Z^m) = m = \deg Q$ (car $b_0 \neq 0$). Par définition du résultant de deux polynômes ([Bou81, A IV.71 §6 Déf. 1]), on a donc $P * Q \in A[X]$. Par ailleurs, supposons que les polynômes P et Q se factorisent sur $\overline{L}$ de la façon suivante

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \quad \text{et} \quad Q(X) = \prod_{j=1}^{m}(X - \beta_j).$$

Alors, on a

$$Q\left(\frac{X}{Z}\right)Z^m = Q(0)\prod_{j=1}^{m}\left(Z - \frac{1}{\beta_j}X\right)$$

et d'après [Bou81, A IV.75 §6 Cor. 1],

$$(P * Q)(X) = Q(0)^n \prod_{i,j}\left(\alpha_i - \frac{1}{\beta_j}X\right).$$

Or, $Q(0) = \prod_{j=1}^{m}(-\beta_j)$, donc

$$(P * Q)(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i\beta_j).$$

C'est la formule de l'énoncé. On en déduit que l'on a :

- $(P * Q)(0) = (-1)^{\deg P \cdot \deg Q} P(0)^{\deg Q} Q(0)^{\deg P} \neq 0$, donc $P * Q \in M_A$;
- $P * P_0 = P_0 * P = P$;
- $P * Q = Q * P$;

De plus, les polynômes $(P * Q) * R$ et $P * (Q * R)$ ont les mêmes racines dans $\overline{L}$ comptées avec multiplicités. Comme ils sont unitaires, ils sont égaux. D'où le lemme.

Pour tout entier $r \geq 1$, on note ζ_r une racine r-ième de l'unité dans $\overline{L}$.

Lemme 4.23 *Soient $r \geq 1$ et $P \in M_A$. Il existe un unique polynôme $P^{(r)} \in M_A$ tel que*

$$P^{(r)}(X^r) = (-1)^{(r+1)\deg P}\prod_{k=0}^{r-1}P(\zeta_r^k X). \tag{4.8}$$

L'application $P \mapsto P^{(r)}$ est un morphisme de monoïdes pour la loi $*$. De plus, si $P \in M_A$ se factorise sur $\overline{L}$ de la façon suivante

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i),$$

on a

$$P^{(r)}(X) = \prod_{i=1}^{n}(X - \alpha_i^r). \tag{4.9}$$

Démonstration. Soit $P \in M_A$. L'unicité d'un polynôme $P^{(r)}$ vérifiant la relation (4.8) étant immédiate, on montre l'existence à partir de la formule proposée. On suppose :

$$\begin{aligned} P(X) &= X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \\ &= \prod_{i=1}^{n}(X - \alpha_i) \quad \text{avec } \alpha_i \in \overline{L}. \end{aligned}$$

On pose alors

$$P^{(r)}(X) = \prod_{i=1}^{n} (X - \alpha_i^r)\,.$$

On doit vérifier :

1. $P^{(r)} \in M_A$;
2. $P^{(r)}(X^r) = (-1)^{(r+1)\deg P} \prod_{k=0}^{r-1} P(\zeta_r^k X)$.

Notons $\{\sigma_k\}_{1\leq k\leq n}$ la famille des polynômes symétriques élémentaires en n variables. Soit k un entier compris entre 1 et n. Le polynôme $\sigma_k(X_1^r, \ldots, X_n^r)$ est symétrique. D'après [Bou81, A IV.58 §6 Th. 1], il existe donc un polynôme $Q_k \in A[Y_1, \ldots, Y_n]$ tel que

$$\sigma_k(X_1^r, \ldots, X_n^r) = Q_k(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)).$$

Donc d'après les relations entre coefficients et racines d'un polynôme, on a

$$\begin{aligned}\sigma_k(\alpha_1^r, \ldots, \alpha_n^r) &= Q_k(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)) \\ &= Q_k(-a_{n-1}, \ldots, (-1)^n a_0) \in A.\end{aligned}$$

Donc $P^{(r)} \in A[X]$. Comme de plus, $P^{(r)}(0) = (-1)^{(r+1)\deg P} P(0)^r \neq 0$ et $P^{(r)}$ est unitaire, on a $P^{(r)} \in M_A$. Vérifions à présent que l'on a bien l'égalité (4.8) :

$$\begin{aligned}P^{(r)}(X^r) = \prod_{i=1}^{n} (X^r - \alpha_i^r) &= \prod_{i=1}^{n} \prod_{k=0}^{r-1} \left(X - \zeta_r^{-k} \alpha_i\right) \\ &= \left(\prod_{k=0}^{r-1} \zeta_r^{-k}\right)^n \prod_{k=0}^{r-1} \prod_{i=1}^{n} \left(\zeta_r^k X - \alpha_i\right) \\ &= \left(\zeta_r^{\frac{r(r-1)}{2}}\right)^{-n} \prod_{k=0}^{r-1} P(\zeta_r^k X).\end{aligned}$$

Or, $\left(\zeta_r^{\frac{r(r-1)}{2}}\right)^2 = \zeta_r^{r(r-1)} = 1$, puis

$$\zeta_r^{\frac{r(r-1)}{2}} = (-1)^{r+1}.$$

On en déduit la formule recherchée et le fait que l'application $P \mapsto P^{(r)}$ est bien définie.

Vérifions enfin qu'il s'agit bien d'un morphisme de monoïdes. On a $P_0^{(r)} = P_0$. Soient P et Q dans M_A. D'après le lemme 4.22 et la formule (4.9), les polynômes $(P * Q)^{(r)}$ et $P^{(r)} * Q^{(r)}$ ont les mêmes racines dans $\overline{L}$ comptées avec multiplicités. Ils sont donc égaux. D'où le lemme 4.23.

Lemme 4.24 *Soient A et B deux anneaux intègres et $\varphi : A \to B$ un morphisme d'anneaux. L'ensemble*

$$M_A^{\varphi} = \{P \in M_A \mid \varphi(P(0)) \neq 0\}$$

est stable pour la loi $*$. *L'application* $\varphi : A[X] \to B[X]$ *définie par*

$$\varphi\big(\sum_i a_i X^i\big) = \sum_i \varphi(a_i) X^i.$$

induit un morphisme de monoïdes (encore noté φ*)*

$$\varphi : M_A^\varphi \longrightarrow M_B.$$

Soient $P \in M_A^\varphi$ *et* $r \geq 1$. *Alors,* $P^{(r)} \in M_A^\varphi$ *et on a*

$$(\varphi(P))^{(r)} = \varphi\big(P^{(r)}\big).$$

Démonstration. D'après le lemme 4.22, si P, $Q \in M_A^\varphi \subset M_A$, on a $P * Q \in M_A$ et

$$(P * Q)(0) = (-1)^{\deg P \cdot \deg Q} P(0)^{\deg Q} Q(0)^{\deg P}.$$

D'où

$$\varphi\left((P * Q)(0)\right) = (-1)^{\deg P \cdot \deg Q} \varphi(P(0))^{\deg Q} \varphi(Q(0))^{\deg P} \neq 0$$

car $\varphi(P(0)) \neq 0$, $\varphi(Q(0)) \neq 0$ et B est intègre. Donc M_A^φ est bien un sous-ensemble de M_A stable pour la loi $*$. On a $\varphi(P_0) = P_0$ et la relation

$$\varphi(P * Q) = \varphi(P) * \varphi(Q), \quad \text{pour } P,\ Q \in M_A^\varphi,$$

résulte de la définition du résultant de deux polynômes ([Bou81, A IV.72 §6]) en termes de déterminant de Sylvester.

Soient $P \in M_A^\varphi$ et $r \geq 1$. Alors, d'après le lemme 4.23, on a $P^{(r)} \in M_A$ et

$$\varphi\big(P^{(r)}(0)\big) = (-1)^{(r+1)\deg P} \varphi(P(0))^r \neq 0$$

car $\varphi(P(0)) \neq 0$ et B est intègre. D'où $P^{(r)} \in M_A^\varphi$. Posons :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = \prod_{i=1}^{n} (X - \alpha_i) \quad \text{avec } \alpha_i \in \overline{L};$$

$$P^{(r)}(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 = \prod_{i=1}^{n} (X - \alpha_i^r) \in A[X];$$

$$\varphi(P)^{(r)}(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \quad \text{avec } c_i \in B.$$

Il s'agit de montrer que pour tout $1 \leq k \leq n$, on a $\varphi(b_{n-k}) = c_{n-k}$. Notons $\{\sigma_k\}_{1 \leq k \leq n}$ la famille des polynômes symétriques élémentaires en n variables. Soit k un entier compris entre 1 et n. Le polynôme $\sigma_k(X_1^r, \ldots, X_n^r)$ est symétrique. D'après [Bou81, A IV.58 §6 Th. 1], il existe donc un unique polynôme $Q_{k,A} \in A[Y_1, \ldots, Y_n]$ (resp. $Q_{k,B} \in B[Y_1, \ldots, Y_n]$) tel que

$$\sigma_k(X_1^r, \ldots, X_n^r) = Q_{k,A}(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n))$$

$$(\text{resp. } \sigma_k(X_1^r, \ldots, X_n^r) = Q_{k,B}(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n))).$$

Donc d'après les relations entre coefficients et racines d'un polynôme, on a

$$\begin{aligned}(-1)^k b_{n-k} = \sigma_k(\alpha_1^r, \ldots, \alpha_n^r) &= Q_{k,A}(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)) \\ &= Q_{k,A}(-a_{n-1}, \ldots, (-1)^n a_0).\end{aligned}$$

Or, par unicité, $\varphi(Q_{k,A}) = Q_{k,B}$. Donc,

$$(-1)^k \varphi(b_{n-k}) = Q_{k,B}(-\varphi(a_{n-1}), \ldots, (-1)^n \varphi(a_0)) = (-1)^k c_{n-k}$$

à nouveau par les relations entre coefficients et racines d'un polynôme. D'où l'égalité $(\varphi(P))^{(r)} = \varphi\big(P^{(r)}\big)$ et le lemme 4.24.

4.3.2 Le polynôme P_ℓ^*

Soit $\prod_{\mathfrak{q}|\ell} \mathfrak{q}^{v_\mathfrak{q}(\ell)}$ la décomposition de l'idéal $\ell\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$. On note g_ℓ le cardinal de l'ensemble $\{\mathfrak{q} \mid \ell\}$. On rappelle que E a par hypothèse bonne réduction en tout idéal premier $\mathfrak{q}$ de $\mathcal{O}_K$ divisant ℓ. Le polynôme P_ℓ^* donné par la formule (4.1) est alors bien défini et à coefficients entiers.

D'après le lemme 4.24, l'application de réduction $\varphi : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ induit un morphisme de monoïdes

$$\begin{array}{ccc} M_\mathbf{Z}^\varphi & \longrightarrow & M_{\mathbf{F}_p} \\ P & \longmapsto & \overline{P}. \end{array}$$

En particulier, $\overline{P * Q} = \overline{P} * \overline{Q}$ pour tout $P, Q \in M_\mathbf{Z}^\varphi$.

Lemme 4.25 *Le polynôme P_ℓ^* appartient à $M_\mathbf{Z}$ et vérifie :*

$$P_\ell^*(0) = \ell^{12 \cdot d \cdot 2^{g_\ell - 1}}. \tag{4.10}$$

Ses racines complexes sont de module ℓ^{6d}. Si de plus $\ell \neq p$, alors $P_\ell^* \in M_\mathbf{Z}^\varphi$ et on a

$$\overline{P_\ell^*}(\Omega) = 0, \quad \text{où} \quad \Omega = \prod_{\mathfrak{q}|\ell} \lambda(\sigma_\mathfrak{q})^{12 v_\mathfrak{q}(\ell)} \in \mathbf{F}_p.$$

Démonstration. Pour tout $\mathfrak{q} \mid \ell$, le polynôme $P_\mathfrak{q}$ est unitaire, à coefficients entiers et vérifie (prop. 4.9) :

$$P_\mathfrak{q}(0) = N(\mathfrak{q}) = \ell^{f_\mathfrak{q}}.$$

En particulier, $P_\mathfrak{q} \in M_\mathbf{Z}$. D'après les lemmes 4.22 et 4.23, le polynôme P_ℓ^* est bien défini (la loi $*$ est associative) et indépendant de l'ordre des idéaux premiers dans la décomposition de ℓ dans K (la loi $*$ est commutative). De plus, P_ℓ^* appartient à $M_\mathbf{Z} \subset \mathbf{Z}[X]$.

Soient $P_1, \ldots, P_n \in M_A$ de degrés respectifs $d_1, \ldots, d_n$. On montre par récurrence sur n, à partir de la formule pour $n = 2$ du lemme 4.22 que l'on a

$$(P_1 * \cdots * P_n)(0) = (-1)^{(n+1)d_1 \cdots d_n} \prod_{i=1}^{n} P_i(0)^{\prod_{j \neq i} d_j}.$$

De plus, d'après le lemme 4.23, pour tout $P \in M_\mathbf{Z}$ et tout entier $r \geq 1$, on a $P^{(r)}(0) = (-1)^{(r+1)\deg P} P(0)^r$. Comme pour tout idéal $\mathfrak{q} \mid \ell$, on a $\deg P_\mathfrak{q} = 2$, on en déduit

$$P_\ell^*(0) = \prod_{\mathfrak{q}|\ell} P_\mathfrak{q}(0)^{12 v_\mathfrak{q}(\ell) \cdot 2^{g_\ell - 1}} = \prod_{\mathfrak{q}|\ell} \big(\ell^{f_\mathfrak{q}}\big)^{12 v_\mathfrak{q}(\ell) \cdot 2^{g_\ell - 1}} = \ell^{12 \cdot 2^{g_\ell - 1} \sum_{\mathfrak{q}|\ell} f_\mathfrak{q} v_\mathfrak{q}(\ell)}.$$

D'où la formule car $\sum_{\mathfrak{q}|\ell} f_\mathfrak{q} v_\mathfrak{q}(\ell) = d$.

Par ailleurs, d'après la proposition 4.9, les racines complexes de $P_{\mathfrak{q}}$ sont de module $N(\mathfrak{q})^{1/2} = \ell^{f_{\mathfrak{q}}/2}$. Donc, d'après le lemme 4.23, celles de $P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(\ell))}$ sont de module $\ell^{6f_{\mathfrak{q}}v_{\mathfrak{q}}(\ell)}$. D'après le lemme 4.22, celles de P_ℓ^* sont de module

$$\prod_{\mathfrak{q}|\ell} \ell^{6f_{\mathfrak{q}}v_{\mathfrak{q}}(\ell)} = \ell^{6\sum_{\mathfrak{q}|\ell} f_{\mathfrak{q}}v_{\mathfrak{q}}(\ell)} = \ell^{6d}.$$

Supposons à présent $\ell \neq p$. Alors, d'après la formule (4.10), on a $P_\ell^* \in M_{\mathbf{Z}}^{\varphi}$. D'après la proposition 4.9, on a

$$\overline{P_{\mathfrak{q}}}(\lambda(\sigma_{\mathfrak{q}})) = 0.$$

Donc d'après le lemme 4.23, on a :

$$\overline{P_{\mathfrak{q}}}^{(12v_{\mathfrak{q}}(\ell))}\left(\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}\right) = 0 \pmod{p}. \tag{4.11}$$

Puis,

$$\begin{aligned}
\overline{P_\ell^*}(\Omega) &= \overline{\underset{\mathfrak{q}|\ell}{*} P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(\ell))}}\Big(\prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}\Big) \\
&= \Big(\underset{\mathfrak{q}|\ell}{*} \overline{P_{\mathfrak{q}}}^{(12v_{\mathfrak{q}}(\ell))}\Big)\Big(\prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}\Big) \quad \text{(lemme 4.24)} \\
&= 0 \pmod{p} \quad \text{(d'après le lemme 4.22 et la relation (4.11))}.
\end{aligned}$$

D'où le lemme 4.25.

4.3.3 Fin de la démonstration du théorème 4.1

On reprend les notations de l'Introduction et des §§4.1–4.2. En particulier, λ désigne le caractère d'isogénie associé à une droite stable.

On rappelle que l'on a supposé $p \geq 5$, non ramifié dans K et pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p, E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2. Il s'agit de montrer que p divise $B_\ell^{(d)}$.

Supposons $p = \ell$. Alors, pour $d \geq 2$, par définition de $B_p^{(d)}$, il existe un entier $k > 0$ tel que $P_p^*(p^{12k})$ divise $B_p^{(d)}$. D'où p divise $B_p^{(d)}$ car

$$\begin{aligned}
P_p^*(p^{12k}) &\equiv P_p^*(0) \pmod{p} \\
&\equiv 0 \pmod{p} \quad \text{d'après le lemme 4.25.}
\end{aligned}$$

Supposons $p \neq \ell$. D'après la proposition 4.20, on a :

$$\Omega = \prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)} = \prod_{\mathfrak{p}|p} N_{\mathfrak{p}}(\ell+\mathfrak{p})^{\alpha_{\mathfrak{p}}}. \tag{4.12}$$

Or, par définition on a

$$\begin{aligned}
N_{\mathfrak{p}}(\ell+\mathfrak{p}) &= \ell^{1+p+\cdots+p^{f_{\mathfrak{p}}-1}} \pmod{p} \\
&= \ell^{f_{\mathfrak{p}}} \pmod{p}
\end{aligned}$$

où $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = \ell^{f_\mathfrak{p}}$. D'où

$$\prod_{\mathfrak{p}|p} N_\mathfrak{p}(\ell + \mathfrak{p})^{\alpha_\mathfrak{p}} = \ell^{\sum_{\mathfrak{p}|p} f_\mathfrak{p}\alpha_\mathfrak{p}}. \tag{4.13}$$

Or, $\alpha_\mathfrak{p} \in \{0, 12\}$ d'après la proposition 4.12 et on pose

$$k = \sum_{\substack{\mathfrak{p}|p \\ \alpha_\mathfrak{p}=12}} f_\mathfrak{p} \geq 0$$

de sorte que

$$\sum_{\mathfrak{p}|p} f_\mathfrak{p}\alpha_\mathfrak{p} = 12k. \tag{4.14}$$

Comme p est non ramifié dans K, on a

$$d = \sum_{\mathfrak{p}|p} f_\mathfrak{p}. \tag{4.15}$$

Or, d'après la remarque suivant la proposition 4.12, on peut toujours, si on le souhaite, remplacer la famille $\{\alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$ par la famille $\{12 - \alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$, donc on peut supposer que l'on a :

$$\sum_{\mathfrak{p}|p} f_\mathfrak{p}\alpha_\mathfrak{p} \leq \sum_{\mathfrak{p}|p} f_\mathfrak{p}(12 - \alpha_\mathfrak{p}).$$

Autrement dit, d'après les égalités (4.14) et (4.15)

$$12k \leq 12(d - k)$$

soit encore

$$k \leq \left[\frac{d}{2}\right].$$

D'après les égalités (4.13) et (4.14) on a

$$\prod_{\mathfrak{p}|p} N_\mathfrak{p}(\ell + \mathfrak{p})^{\alpha_\mathfrak{p}} = \ell^{12k} \pmod{p}. \tag{4.16}$$

Par ailleurs, d'après le lemme 4.25, on a

$$\overline{P_\ell^*}(\Omega) = 0.$$

Donc, d'après les égalités (4.12) et (4.16), il vient

$$\overline{P_\ell^*}\left(\ell^{12k}\right) = 0$$

c'est-à-dire

$$P_\ell^*\left(\ell^{12k}\right) \equiv 0 \pmod{p}.$$

D'où le théorème 4.1.

4.4 Démonstration de la proposition 4.4

On considère la famille $\{T_n\}_{n\geq 1}$ des polynômes de Tchebychev. En particulier, on a

$$T_3(X) = 4X^3 - 3X; \quad 1 - T_3(X) = -(X-1)(2X+1)^2;$$
$$1 + T_3(X) = (X+1)(2X-1)^2; \quad 2T_3(X)^2 - 1 = (2X^2-1)(16X^4 - 16X^2 + 1).$$

On rappelle que pour tout entier $n \geq 1$, on a :

$$1 - T_{2n}(X) = 2\left(1 - T_n(X)^2\right) \quad \text{ou encore} \quad 1 + T_{2n}(X) = 2T_n(X)^2. \tag{4.17}$$

Soit ℓ nombre premier tel que E a bonne réduction en chaque idéal premier de $\mathcal{O}_K$ divisant ℓ. On distingue trois cas selon la décomposition de ℓ dans K.

1. Supposons ℓ ramifié dans K avec $\ell\mathcal{O}_K = \mathfrak{q}^2$ et posons

$$P_{\mathfrak{q}}(X) = X^2 - t_{\mathfrak{q}}X + \ell = (X-\alpha)(X-\beta).$$

D'après la prop. 4.9, on a $|\alpha| = |\beta| = \sqrt{\ell}$. Posons donc $\alpha = \sqrt{\ell}e^{i\theta}$ avec $\theta \in \mathbf{R}$. D'après le lemme 4.22, on a

$$P_\ell^*(X) = (X - \alpha^{24})(X - \beta^{24}).$$

D'où

$$\begin{aligned} P_\ell^*(X) &= X^2 - (\alpha^{24} + \beta^{24})X + \ell^{24} \\ &= X^2 - 2\ell^{12}\cos(24\theta)X + \ell^{24}. \end{aligned}$$

Or, $\cos(24\theta) = T_{24}(\cos\theta)$ et $2\sqrt{\ell}\cos\theta = t_{\mathfrak{q}}$, d'où

$$\begin{aligned} P_\ell^*(X) &= X^2 - 2\ell^{12}T_{24}\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right)X + \ell^{24} \\ &= (X-\ell^{12})^2 + 2\ell^{12}\left(1 - T_{24}\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right)\right)X. \end{aligned}$$

On en déduit immédiatement

$$P_\ell^*(\ell^{12}) = 2\ell^{24}\left(1 - T_{24}\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right)\right).$$

Or, d'après les relations (4.17), on a

$$1 - T_{24} = 2^5(1-T_3)(1+T_3)T_3^2(2T_3^2-1)^2.$$

D'où la factorisation

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_{\mathfrak{q}}^2(t_{\mathfrak{q}}^2-\ell)^2(t_{\mathfrak{q}}^2-4\ell)(t_{\mathfrak{q}}^2-2\ell)^2(t_{\mathfrak{q}}^2-3\ell)^2(t_{\mathfrak{q}}^4-4\ell t_{\mathfrak{q}}^2+\ell^2)^2$$

car

$$T_3\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right) = \frac{t_{\mathfrak{q}}}{2\ell\sqrt{\ell}}\left(t_{\mathfrak{q}}^2 - 3\ell\right);$$
$$1 - T_3\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right) = -\frac{1}{2\ell\sqrt{\ell}}(t_{\mathfrak{q}} - 2\sqrt{\ell})(t_{\mathfrak{q}} + \sqrt{\ell})^2;$$
$$1 + T_3\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right) = \frac{1}{2\ell\sqrt{\ell}}(t_{\mathfrak{q}} + 2\sqrt{\ell})(t_{\mathfrak{q}} - \sqrt{\ell})^2;$$
$$2T_3\left(\frac{t_{\mathfrak{q}}}{2\sqrt{\ell}}\right)^2 - 1 = \frac{1}{2\ell^3}(t_{\mathfrak{q}}^2 - 2\ell)(t_{\mathfrak{q}}^4 - 4\ell t_{\mathfrak{q}}^2 + \ell^2).$$

On en déduit que l'on a $P_\ell^*(\ell^{12}) = 0$ si et seulement si

(a) soit $\ell \geq 5$ et $t_\mathfrak{q} = 0$;

(b) soit $\ell = 3$ et $t_\mathfrak{q} = 0$ ou ± 3 ;

(c) soit $\ell = 2$ et $t_\mathfrak{q} = 0$ ou ± 2.

Autrement dit, si et seulement si $t_\mathfrak{q} \equiv 0 \pmod{\ell}$ car $|t_\mathfrak{q}| \leq 2\sqrt{\ell}$.

2. Supposons ℓ inerte dans K avec $\ell\mathcal{O}_K = \mathfrak{q}$ et posons

$$P_\mathfrak{q}(X) = X^2 - t_\mathfrak{q} X + \ell^2 = (X - \alpha)(X - \beta).$$

D'après la prop. 4.9, on a $|\alpha| = |\beta| = \ell$. Posons donc $\alpha = \ell e^{i\theta}$ avec $\theta \in \mathbf{R}$. D'après le lemme 4.22, on a

$$P_\ell^*(X) = (X - \alpha^{12})(X - \beta^{12}).$$

D'où

$$\begin{aligned} P_\ell^*(X) &= X^2 - (\alpha^{12} + \beta^{12})X + \ell^{24} \\ &= X^2 - 2\ell^{12}\cos(12\theta)X + \ell^{24}. \end{aligned}$$

Or, $\cos(12\theta) = T_{12}(\cos\theta)$ et $2\ell\cos\theta = t_\mathfrak{q}$, d'où

$$\begin{aligned} P_\ell^*(X) &= X^2 - 2\ell^{12}T_{12}\left(\frac{t_\mathfrak{q}}{2\ell}\right)X + \ell^{24} \\ &= (X - \ell^{12})^2 + 2\ell^{12}\left(1 - T_{12}\left(\frac{t_\mathfrak{q}}{2\ell}\right)\right)X. \end{aligned}$$

On en déduit immédiatement

$$P_\ell^*(\ell^{12}) = 2\ell^{24}\left(1 - T_{12}\left(\frac{t_\mathfrak{q}}{2\ell}\right)\right).$$

Or, d'après les relations (4.17), on a

$$1 - T_{12} = 8(1 - T_3)(1 + T_3)T_3^2.$$

D'où la factorisation

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_\mathfrak{q}^2(t_\mathfrak{q}^2 - \ell^2)^2(t_\mathfrak{q}^2 - 4\ell^2)(t_\mathfrak{q}^2 - 3\ell^2)^2$$

car

$$\begin{aligned} T_3\left(\frac{t_\mathfrak{q}}{2\ell}\right) &= \frac{t_\mathfrak{q}}{2\ell^3}\left(t_\mathfrak{q}^2 - 3\ell^2\right); \\ 1 - T_3\left(\frac{t_\mathfrak{q}}{2\ell}\right) &= -\frac{1}{2\ell^3}(t_\mathfrak{q} - 2\ell)(t_\mathfrak{q} + \ell)^2; \\ 1 + T_3\left(\frac{t_\mathfrak{q}}{2\ell}\right) &= \frac{1}{2\ell^3}(t_\mathfrak{q} + 2\ell)(t_\mathfrak{q} - \ell)^2. \end{aligned}$$

On en déduit que l'on a $P_\ell^*(\ell^{12}) = 0$ si et seulement si $t_\mathfrak{q} = 0$, $\pm\ell$ ou $\pm 2\ell$. Autrement dit, si et seulement si $t_\mathfrak{q} \equiv 0 \pmod{\ell}$ car $|t_\mathfrak{q}| \leq 2\ell$.

3. Supposons ℓ décomposé dans K avec $\ell\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ et posons

$$P_{\mathfrak{q}_j}(X) = X^2 - t_{\mathfrak{q}_j}X + \ell = (X-\alpha_j)(X-\beta_j), \quad \text{avec } j = 1, 2.$$

D'après la prop. 4.9, on a $|\alpha_j| = |\beta_j| = \ell$. Posons donc $\alpha_j = \ell e^{i\theta_j}$ avec $\theta_j \in \mathbf{R}$. D'après le lemme 4.22, on a

$$P_\ell^*(X) = (X - \alpha_1^{12}\alpha_2^{12})(X - \alpha_1^{12}\beta_2^{12})(X - \beta_1^{12}\alpha_2^{12})(X - \beta_1^{12}\beta_2^{12}).$$

D'où

$$P_\ell^*(X) = (X^2 - 2\ell^{12}\cos(12(\theta_1+\theta_2))X + \ell^{24})(X^2 - 2\ell^{12}\cos(12(\theta_1-\theta_2))X + \ell^{24}).$$

Or,

$$\begin{cases} \cos(12(\theta_1+\theta_2)) + \cos(12(\theta_1-\theta_2)) &= 2\cos(12\theta_1)\cos(12\theta_2) \\ \cos(12(\theta_1+\theta_2)) \cdot \cos(12(\theta_1-\theta_2)) &= \cos^2(12\theta_1) + \cos^2(12\theta_2) - 1 \end{cases}$$

et $\cos(12\theta_j) = T_{12}(\cos\theta_j)$ et $2\sqrt{\ell}\cos\theta_j = t_{\mathfrak{q}_j}$. D'où

$$\begin{aligned} P_\ell^*(X) &= X^4 - 4\ell^{12}T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)X^3 + 2\ell^{24}\left(2T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)^2\right. \\ &\quad \left. + 2T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)^2 - 1\right)X^2 - 4\ell^{36}T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)X + \ell^{48} \\ &= (X^2 - \ell^{24})^2 - 4\ell^{12}\left(T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)X^2 - \ell^{12}\left(T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)^2\right.\right. \\ &\quad \left.\left. + T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)^2\right)X + \ell^{24}T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)\right)X. \end{aligned}$$

C'est bien la formule de l'énoncé. On en déduit immédiatement

$$P_\ell^*(\ell^{12}) = 4\ell^{48}\left(T_{12}\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right) - T_{12}\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)\right)^2.$$

Or, d'après les relations (4.17), on a

$$\begin{aligned} T_{12}(X) - T_{12}(Y) &= 4(T_3(X) - T_3(Y))(T_3(X) + T_3(Y))(T_6(X) + T_6(Y)) \\ &= 8(T_3(X) - T_3(Y))(T_3(X) + T_3(Y))(T_3(X)^2 + T_3(Y)^2 - 1). \end{aligned}$$

De plus,

$$\begin{aligned} T_3\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right) - T_3\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right) &= \frac{1}{2\ell\sqrt{\ell}}(t_{\mathfrak{q}_1} - t_{\mathfrak{q}_2})(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 + t_{\mathfrak{q}_1}t_{\mathfrak{q}_2} - 3\ell); \\ T_3\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right) + T_3\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right) &= \frac{1}{2\ell\sqrt{\ell}}(t_{\mathfrak{q}_1} + t_{\mathfrak{q}_2})(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - t_{\mathfrak{q}_1}t_{\mathfrak{q}_2} - 3\ell); \end{aligned}$$

et

$$T_3\left(\frac{t_{\mathfrak{q}_1}}{2\sqrt{\ell}}\right)^2 + T_3\left(\frac{t_{\mathfrak{q}_2}}{2\sqrt{\ell}}\right)^2 - 1 = \frac{1}{\ell^3}(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 4\ell)\left((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - \ell)^2 - 3t_{\mathfrak{q}_1}^2 t_{\mathfrak{q}_2}^2\right).$$

D'où la factorisation

$$P_\ell^*(\ell^{12}) = \ell^{36}\left(t_{\mathfrak{q}_1}^2 - t_{\mathfrak{q}_2}^2\right)^2\left((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 3\ell)^2 - t_{\mathfrak{q}_1}^2 t_{\mathfrak{q}_2}^2\right)^2\left(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 4\ell\right)^2 \times \left((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - \ell)^2 - 3t_{\mathfrak{q}_1}^2 t_{\mathfrak{q}_2}^2\right)^2.$$

On en déduit que l'on a $P_\ell^*(\ell^{12}) = 0$ si et seulement si l'une des conditions suivantes est satisfaite :

$$t_{\mathfrak{q}_1} = \pm t_{\mathfrak{q}_2}; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 \pm t_{\mathfrak{q}_1} t_{\mathfrak{q}_2} = 3\ell; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 = 4\ell.$$

Cela achève la démonstration de la proposition 4.4.

4.5 Bornes uniformes

4.5.1 Démonstration de la proposition 4.5

Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ tel que le sous-groupe $\Phi_\mathfrak{q}$ soit non cyclique. Compte-tenu de la structure des groupes Φ, l'idéal premier $\mathfrak{q}$ a nécessairement caractéristique résiduelle $\ell = 2$ ou 3 ([Ser72, §5.6(*a*)]) et $|\Phi_\mathfrak{q}| = 8$ ou 24 (resp. 12) si $\ell = 2$ (resp. $\ell = 3$). L'irréductibilité de ρ_p résulte alors de la proposition 4.15. On peut également invoquer le lemme 4.26 ci-dessous et le fait que $\Phi_\mathfrak{q}$ se plonge dans $\mathrm{Aut}(E[p])$ (car $\ell \neq p$ et $p \geq 3$, [Ser72, §5.6(*a*)]).

Notation. On rappelle qu'un sous-groupe maximal de $\mathrm{Aut}(E[p])$ stabilisant une droite de $E[p]$ est appelé sous-groupe de Borel.

Lemme 4.26 *Soit H un sous-groupe de $\mathrm{Gal}(K(E[p])/K)$. On suppose H non abélien fini. Si p ne divise pas l'ordre de H, alors H ne se plonge pas dans un sous-groupe de Borel de $\mathrm{Aut}(E[p])$.*

Démonstration. Supposons qu'il existe un morphisme injectif ι de G dans un sous-groupe de Borel B de $\mathrm{Aut}(E[p])$. Dans une base convenable de $E[p]$ sur $\mathbf{F}_p$, B est représentable matriciellement par le Borel standard

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Il contient alors le sous-groupe S d'ordre p engendré par l'élément

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

C'est un sous-groupe distingué de B. Comme l'ordre de H est premier à p, le morphisme composé

$$H \overset{\iota}{\hookrightarrow} B \to B/S$$

est injectif. Par ailleurs, B/S est abélien. D'où une contradiction car H est supposé non abélien.

4.5.2 Démonstration de la proposition 4.6

Soient $p \geq 3$ un nombre premier exceptionnel et $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ de caractéristique résiduelle $\ell \neq p$ en lequel E a mauvaise réduction additive avec potentiellement bonne réduction. On souhaite montrer qu'il existe un entier $n \geq 0$ tel que l'ordre du groupe $\Phi_\mathfrak{q}$ divise $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$.

Vu la théorie du corps de classes, le caractère λ s'interprète comme un homomorphisme

$$\lambda : \mathrm{Gal}(K^\mathfrak{m}/K) \longrightarrow \mathbf{F}_p^*,$$

où $\mathfrak{m}$ est le conducteur de λ et $K^\mathfrak{m}$ le corps de classes de rayon $\mathfrak{m}$. Alors, d'après les propositions 4.14 et 4.15, le caractère λ est ramifié en $\mathfrak{q}$ et on a une factorisation du type

$$\mathfrak{m} = \mathfrak{m}' \cdot \mathfrak{q}^{n+1}, \quad \text{où } n \geq 0 \quad \text{ et } (\mathfrak{m}', \mathfrak{q}) = 1.$$

L'ordre du groupe $\Phi_\mathfrak{q}$ divise l'indice de ramification en $\mathfrak{q}$ de l'extension $K^\mathfrak{m}/K$. Or l'extension intermédiaire $K^{\mathfrak{m}'}/K$ est non ramifiée en $\mathfrak{q}$. Donc l'ordre de $\Phi_\mathfrak{q}$ divise le cardinal du groupe $\mathrm{Gal}(K^\mathfrak{m}/K^{\mathfrak{m}'})$. Notons $h_\mathfrak{m}$ (resp. $h_{\mathfrak{m}'}$) le cardinal du groupe $\mathrm{Gal}(K^\mathfrak{m}/K)$ (resp. $\mathrm{Gal}(K^{\mathfrak{m}'}/K)$). Alors, d'après [Coh00, cor.3.2.4], on a

$$|\mathrm{Gal}(K^\mathfrak{m}/K^{\mathfrak{m}'})| = \frac{h_\mathfrak{m}}{h_{\mathfrak{m}'}} = \frac{(\mathcal{U} : \mathcal{U}_{\mathfrak{m}',1})}{(\mathcal{U} : \mathcal{U}_{\mathfrak{m},1})} N(\mathfrak{q})^n(N(\mathfrak{q})-1),$$

où $\mathcal{U}_{\mathfrak{m},1}$ (resp. $\mathcal{U}_{\mathfrak{m}',1}$) désigne le sous-groupe du groupe des unités $\mathcal{U}$ de $\mathcal{O}_K$ qui sont congrues à 1 modulo $\mathfrak{m}$ (resp. $\mathfrak{m}'$) au sens de [Coh00, Def.3.2.2]. Or, comme $\mathfrak{m}'$ divise $\mathfrak{m}$, l'indice de $\mathcal{U}_{\mathfrak{m}',1}$ dans $\mathcal{U}$ divise celui de $\mathcal{U}_{\mathfrak{m},1}$. Donc, l'ordre de $\mathrm{Gal}(K^\mathfrak{m}/K^{\mathfrak{m}'})$ divise $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$ et il en va de même en particulier pour l'ordre de $\Phi_\mathfrak{q}$. D'où la proposition 4.6.

Remarque. Lorsque $\ell \geq 5$, on a $|\Phi_\mathfrak{q}| = 2$, 3, 4 ou 6 ([Ser72, p. 312]). Or $N(\mathfrak{q})$ est premier à 12, donc $|\Phi_\mathfrak{q}|$ divise $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$ pour un certain entier n si et seulement si $|\Phi_\mathfrak{q}|$ divise $N(\mathfrak{q})-1$. Cela justifie la remarque après la proposition 4.6.

4.5.3 Démonstration des corollaires 4.7 et 4.8

Supposons que $\mathfrak{q}$ divise 2. Lorsque $|\Phi_\mathfrak{q}| = 8$ ou 24, le groupe $\Phi_\mathfrak{q}$ n'est pas abélien ([Ser72, 5.6(a)]) et la conclusion résulte de la prop. 4.5. Pour $|\Phi_\mathfrak{q}| = 3$ ou 6, supposons la représentation ρ_p réductible. Alors, d'après la prop. 4.6, l'ordre de $\Phi_\mathfrak{q}$ divise $2^{f_\mathfrak{q}}(2^{f_\mathfrak{q}}-1)$. Or, $2^{f_\mathfrak{q}} - 1 \equiv 1 \pmod 3$ car $f_\mathfrak{q}$ est impair. D'où une contradiction et le corollaire 4.7.

Supposons que $\mathfrak{q}$ divise 3. Lorsque $|\Phi_\mathfrak{q}| = 12$, le groupe $\Phi_\mathfrak{q}$ n'est pas abélien ([Ser72, 5.6(a)]) et la conclusion résulte comme ci-dessus de la prop. 4.5. Pour $|\Phi_\mathfrak{q}| = 4$, supposons la représentation ρ_p réductible. Alors, d'après la prop. 4.6, l'ordre de $\Phi_\mathfrak{q}$ divise $3^{f_\mathfrak{q}}(3^{f_\mathfrak{q}}-1)$. Or, $3^{f_\mathfrak{q}} - 1 \equiv 2 \pmod 4$ car $f_\mathfrak{q}$ est impair, d'où une contradiction et le corollaire 4.8.

4.6 Exemples numériques

Étant donnée une courbe elliptique E, on désigne par $\mathrm{Exc}(E)$ l'ensemble de ses nombres premiers exceptionnels. L'objet de cette section est de déterminer

explicitement, pour certaines courbes elliptiques E définies sur des corps de nombres, l'ensemble $\mathrm{Exc}(E)$.

4.6.1 Stratégie

Pour chacune des courbes considérées, on commence par déterminer son type de réduction en chaque idéal premier. Si pour l'un d'entre eux, on est dans un cas d'application des « résultats uniformes » (prop. 4.5 et 4.6 et cor. 4.7 et 4.8) du §4.1, il ne reste plus alors à traiter que le cas $p = 2$ et éventuellement $p = 3$ et $p = \ell$ où ℓ est un nombre premier ≥ 5. Sinon, on applique le critère du théorème 4.1. On cherche alors un nombre premier ℓ de « bonne réduction » pour lequel $B_\ell^{(d)}$ soit non nul. Si d est impair, c'est automatique (cor. 4.3). Si d est pair il faut et il suffit que l'on ait $P_\ell^*(\ell^{6d}) \neq 0$. Bien que l'on ne sache pas montrer que pour une courbe sans multiplication complexe, il existe toujours un tel nombre premier, cela ne pose aucun problème d'en trouver un dans la pratique. Après quelques itérations du théorème 4.1, on obtient alors un ensemble très restreint de nombres premiers contenant 2, 3 et les premiers ramifiés dans le corps. On traite alors « à la main » ceux qui restent. Soit on trouve un idéal premier $\mathfrak{q}$ de bonne réduction ne divisant pas p tel que $P_\mathfrak{q}$ soit irréductible modulo p et alors p n'est pas exceptionnel, soit on montre que E possède un sous-groupe stable d'ordre p et alors p est exceptionnel.

4.6.2 Notations

La courbe E est donnée sous forme d'une équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_i \in \mathcal{O}_K$. On adopte les notations standard de Tate ([Tat75]). Pour chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on note $v_\mathfrak{p}$ la valuation en $\mathfrak{p}$ de K normalisée par $v_\mathfrak{p}(K^*) = \mathbf{Z}$.

Étant donné un nombre premier ℓ, on note $\mathfrak{S}_\ell^{(d)}$ l'ensemble des diviseurs premiers de $B_\ell^{(d)}$. Lorsque E est définie sur un corps quadratique, on dispose de deux programmes `pari` : l'un, `TraceOfFrobenius`, permet de calculer la famille $\{t_\mathfrak{q}\}_{\mathfrak{q}|\ell}$; l'autre, `ExceptionalPrimes`, de déterminer l'ensemble $\mathfrak{S}_\ell^{(2)}$ (et aussi l'entier $B_\ell^{(2)}$).

4.6.3 Corps quadratiques

On suppose que K est un corps quadratiques, *i.e.* $d = 2$.

Courbes semi-stables et corps quadratiques

Dans le cas où $\mathcal{E}$ est l'ensemble des courbes semi-stables, Kraus a obtenu plusieurs résultats en direction de la question 2 ([Kra96, Kra07]). Dans le cas des corps quadratiques, il montre notamment le résultat suivant ([Kra96, th. p.246]) en utilisant les bornes de Merel ([Mer96]) sur les points de torsion des courbes elliptiques sur les corps de nombres.

Théorème 4.27 (Kraus) *Soit K un corps quadratique. Il existe une constante effective $c(K)$ ne dépendant que de K telle que pour toute courbe elliptique* semi-stable *E définie sur K et pour tout nombre premier $p > c(K)$, la représentation ρ_p est irréductible.*

Remarque. D'après un résultat non publié de Oesterlé et en suivant la démonstration de *loc. cit.*, on montre que l'on peut choisir

$$c(K) = \max\left(\left(1 + 3^{h_K^+}\right)^2, D_K \cdot M(K)\right),$$

où h_K^+ est le nombre de classes de K au sens restreint et

$$M(K) = \begin{cases} 1 & \text{si } K \text{ est imaginaire;} \\ N_{K/\mathbf{Q}}(u^2 - 1) & \text{si } K \text{ est réel d'unité fondamentale } u. \end{cases}$$

Courbes non semi-stables et corps quadratiques

Exemple 4.28 *On suppose $K = \mathbf{Q}(\sqrt{5})$. On considère la courbe E d'équation*

$$y^2 = x^3 + 2x^2 + \omega x \quad \text{où} \quad \omega = \frac{1+\sqrt{5}}{2}.$$

Alors, $\mathrm{Exc}(E) = \{2\}$ *et* $(0,0)$ *est un point d'ordre* 2.

Démonstration. On a

$$\begin{cases} c_4 = 2^4(4 - 3\omega) \\ c_6 = 2^6(-8 + 9\omega) \\ \Delta = -2^6\omega. \end{cases}$$

Or, ω est une unité de $\mathcal{O}_K$. En particulier, la courbe E a bonne réduction en dehors de (l'idéal premier) $2\mathcal{O}_K$. On a :

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 6).$$

Donc E a mauvaise réduction additive en 2. On note Φ_2 son défaut de semi-stabilité en 2. On a $v_2(j) = 6$ et $3v_2(c_4) = 2v_2(c_6)$. L'extension $K/\mathbf{Q}$ étant non ramifié en 2, on a d'après [Cal04], $|\Phi_2| = 4$ ou 8. Or, avec les notations de *loc. cit.* la condition (C2) n'est pas satisfaite. On en déduit que l'on a $|\Phi_2| = 8$. Et, d'après le cor. 4.7, ρ_p est irréductible pour tout nombre premier $p \geq 5$. La courbe E a bonne réduction en l'idéal premier $7\mathcal{O}_K$ et d'après le programme `TraceOfFrobenius`, on a $t_7 = -12$. D'où

$$P_7(X) = X^2 - t_7X + 49 \equiv X^2 + 1 \pmod 3.$$

Donc ρ_3 est également irréductible. La représentation ρ_2, en revanche, est réductible car $(0,0)$ est un point d'ordre 2.

Exemple 4.29 *On suppose $K = \mathbf{Q}(\sqrt{-3})$. On considère la courbe E d'équation*

$$y^2 = x^3 + x + 1 + 2\omega, \quad \text{où} \quad \omega = \frac{1+\sqrt{-3}}{2}.$$

Alors, l'ensemble $\mathrm{Exc}(E)$ *est vide.*

Démonstration. On a

$$\begin{cases} c_4 = -2^4 \cdot 3 \\ c_6 = -2^5 \cdot 3^3(1+2\omega) \\ \Delta = 2^4(77-216\omega). \end{cases}$$

En particulier, $N_{K/\mathbf{Q}}(\Delta) = 2^8 \cdot 157 \cdot 229$ et, ni 157, ni 229 ne divisent c_4. Donc la courbe E a mauvaise réduction multiplicative en un idéal premier au-dessus de 157 et en un idéal premier au-dessus de 229 (157 et 229 sont tous deux décomposés dans K). Par ailleurs, l'idéal $2\mathcal{O}_K$ est premier et

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 5, 4).$$

En particulier, E a mauvaise réduction additive en 2 avec potentiellement bonne réduction. Comme $v_2(j) = 8$, on a d'après [Cal04], $|\Phi_2| = 3$, 6 ou 24. Or,

$$j' = \frac{j}{2^8} \equiv 1 \pmod 4$$

donc pour tout $\gamma \in \{1, \omega, \omega^2\}$, $j' \not\equiv \gamma^4 + 2\gamma^3 \pmod 4$. Autrement dit, avec les notations de *loc. cit.*, la condition (C3) n'est pas satisfaite. On en déduit que l'on a $|\Phi_2| = 24$. Donc d'après le cor. 4.7, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$. Il ne reste plus qu'à traiter les cas $p = 2$ et $p = 3$. La courbe E a bonne réduction en chacun des idéaux premiers divisant 7 et 11 et d'après le programme `TraceOfFrobenius`, on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|7} = \{0, -2\} \quad \text{et} \quad t_{11} = -5.$$

Donc le polynôme

$$P_{11}(X) = X^2 + 5X + 11^2$$

est irréductible modulo 2. Et, si $\mathfrak{p}_7$ désigne l'idéal premier de $\mathcal{O}_K$ au-dessus de 7 tel que $t_{\mathfrak{p}_7} = 0$, le polynôme

$$P_{\mathfrak{p}_7}(X) = X^2 + 7$$

est irréductible modulo 3. On en déduit le résultat annoncé.

Exemple 4.30 *On suppose $K = \mathbf{Q}(\sqrt{13})$. On considère la courbe E d'équation*

$$y^2 = x^3 - (313 + 240\omega)x - 17 \quad \textit{où} \quad \omega = \frac{1+\sqrt{13}}{2}.$$

Alors, l'ensemble $\mathrm{Exc}(E)$ *est vide.*

Démonstration. On a

$$\begin{cases} c_4 = 2^4 \cdot 3(11+8\omega)^2 \\ c_6 = 2^5 \cdot 3^3 \cdot 17 \\ \Delta = 2^4 \cdot 5(11+8\omega)^2(213629 + 167568\omega). \end{cases}$$

De plus, $N_{K/\mathbf{Q}}(213629 + 167568\omega) = -1153 \cdot 2430503$ et ni 1153, ni 2430503 ne divisent c_4. Donc la courbe E a mauvaise réduction multiplicative en un idéal premier au-dessus de 1153 et un idéal premier au-dessus de 2430503. Le nombre premier 2 est inerte dans K et

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 5, 4).$$

Donc $v_2(j) = 8$ et d'après [Cal04], on a $|\Phi_2| = 3$, 6 ou 24. Comme par ailleurs,

$$j' = \frac{j}{2^8} \equiv -1 \pmod 4,$$

la condition (C3) de *loc. cit.* est satisfaite avec $\gamma = 1$ et $|\Phi_2| = 3$ ou 6 (en fait $|\Phi_2| = 6$ d'après *loc. cit.*). Puisque $f_2 = 2$ est pair, le cor. 4.7 ne s'applique pas. Cependant, en l'idéal premier $\mathfrak{p}_{17} = (15 + 4\sqrt{13})\mathcal{O}_K$, on a

$$(v_{\mathfrak{p}_{17}}(c_4), v_{\mathfrak{p}_{17}}(c_6), v_{\mathfrak{p}_{17}}(\Delta)) = (2, 1, 2).$$

Donc E a mauvaise réduction additive en $\mathfrak{p}_{17}$ avec potentiellement bonne réduction. Son défaut de semi-stabilité $\Phi_{\mathfrak{p}_{17}}$ est d'ordre 6 ([Ser72, p.312]). Or, 6 ne divise pas $N(\mathfrak{p}_{17}) - 1 = 16$. Donc, d'après la prop. 4.6, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 3$ et $p \neq 17$. Si $\mathfrak{p}_3$ désigne un idéal divisant 3, alors E a bonne réduction en $\mathfrak{p}_3$ et d'après le programme `TraceOfFrobenius`, on a

$$t_{\mathfrak{p}_3} = -3.$$

Donc le polynôme $P_{\mathfrak{p}_3}(X) = X^2 + 3X + 3$ est irréductible modulo 2 et 17. On en déduit le résultat.

Exemple 4.31 *On suppose $K = \mathbf{Q}(\sqrt{-1})$. Pour tout entier $a \in \mathbf{Z}[\sqrt{-1}]$, on considère la courbe E_a d'équation*

$$y^2 = x^3 + ax + a.$$

Supposons que l'on ait $v_{\mathfrak{p}_2}(a) = 0, 1, 3, 4, 5, 6$ ou 7, où $\mathfrak{p}_2$ est l'unique idéal de $\mathcal{O}_K$ au-dessus de 2. Alors, l'ensemble $\mathrm{Exc}(E_a)$ *est contenu dans* $\{2, 3\}$.

Démonstration. On a

$$\begin{cases} c_4(E_a) = -2^4 \cdot 3 \cdot a \\ c_6(E_a) = -2^5 \cdot 3 \cdot a \\ \Delta(E_a) = -2^4 \cdot a^2(4a + 27). \end{cases}$$

En particulier, $v_{\mathfrak{p}_2}(c_4(E_a)) = 8 + v_{\mathfrak{p}_2}(a)$, $v_{\mathfrak{p}_2}(\Delta(E_a)) = 8 + 2v_{\mathfrak{p}_2}(a)$ et

$$v_{\mathfrak{p}_2}(j(E_a)) = 16 + v_{\mathfrak{p}_2}(a) \geq 0.$$

Donc E_a a mauvaise réduction additive en $\mathfrak{p}_2$ avec potentiellement bonne réduction. Par ailleurs, 2 est ramifié dans K (donc $f_{\mathfrak{p}_2} = 1$ est impair) et

$$v_{\mathfrak{p}_2}(j(E_a)) \in \{16, 17, 19, 20, 21, 22, 23\}.$$

Donc, d'après [Bil08b], on a $|\Phi_{\mathfrak{p}_2}| \in \{3, 6, 8, 24\}$. On conclut avec le cor. 4.7.

Avec les notations de l'exemple précédent, lorsque $v_{\mathfrak{p}_2}(a) = 2$ ou ≥ 8, le corollaire 4.7 ne s'applique pas toujours. On traite ci-dessous un exemple dans le cas où $v_{\mathfrak{p}_2}(a) = 2$.

Exemple 4.32 *On suppose $K = \mathbf{Q}(\sqrt{-1})$. On considère la courbe E d'équation*

$$y^2 = x^3 + 2(3 + 2\sqrt{-1})x + 2(3 + 2\sqrt{-1}). \tag{4.18}$$

Alors, l'ensemble $\mathrm{Exc}(E)$ *est vide.*

Démonstration. On a

$$\begin{cases} c_4 = -2^5 \cdot 3(3+2\sqrt{-1}) \\ c_6 = -2^6 \cdot 3^3(3+2\sqrt{-1}) \\ \Delta = -2^6(3+2\sqrt{-1})^2 \cdot (51+16\sqrt{-1}). \end{cases}$$

On a $2\mathcal{O}_K = \mathfrak{p}_2^2$ où $\mathfrak{p}_2 = (1+\sqrt{-1})\mathcal{O}_K$ et

$$(v_{\mathfrak{p}_2}(c_4), v_{\mathfrak{p}_2}(c_6), v_{\mathfrak{p}_2}(\Delta)) = (10, 12, 12).$$

Donc, d'après [Pap93], l'équation (4.18) correspond à un cas 6 ou 7 de Tate. En particulier, il est minimal en $\mathfrak{p}_2$ et E a réduction additive en $\mathfrak{p}_2$. Déterminons à présent l'ordre $|\Phi_{\mathfrak{p}_2}|$ de son défaut de semi-stabilité en $\mathfrak{p}_2$. On a $v_{\mathfrak{p}_2}(j) = 18$ et $\pi = 1+\sqrt{-1}$ est une uniformisante de $K_{\mathfrak{p}_2}$. De plus,

$$\frac{c_4}{\pi^{10}} \equiv 1 + \pi \pmod 2.$$

Donc, d'après [Bil08b, th.2], on a $|\Phi_{\mathfrak{p}_2}| = 4$. On ne peut donc pas appliquer le cor. 4.7.

Notons $\mathfrak{p}_{13}$ l'idéal premier de $\mathcal{O}_K$ engendré par $3+2\sqrt{-1}$. On a

$$(v_{\mathfrak{p}_{13}}(c_4), v_{\mathfrak{p}_{13}}(\Delta)) = (1, 2),$$

d'où $v_{\mathfrak{p}_{13}}(j) = 1$. L'équation (4.18) est minimale en $\mathfrak{p}_{13}$ et E a mauvaise réduction additive en $\mathfrak{p}_{13}$ avec potentiellement bonne réduction. Son défaut de semi-stabilité est d'ordre 6 (*c.f.* [Ser72, p.312]). Comme 6 divise $N(\mathfrak{p}_{13}) - 1 = 12$, la prop. 4.6 ne donne aucune majoration de $\mathrm{Exc}(E)$. Par ailleurs, on a $v_{\mathfrak{p}_{13}}(\Delta) = 2$ et d'après [Kra97a, lem.1] (ou la prop. 4.18), E n'a pas potentiellement bonne réduction de hauteur 2 en $\mathfrak{p}_{13}$.

Notons $\mathfrak{p}_{2857}$ l'idéal premier de $\mathcal{O}_K$ engendré par $51+16\sqrt{-1}$. La courbe E a mauvaise réduction multiplicative en $\mathfrak{p}_{2857}$. En dehors de $\mathfrak{p}_2$, $\mathfrak{p}_{13}$ et $\mathfrak{p}_{2857}$, la courbe E a bonne réduction.

Vu l'étude précédente, aucun des résultats « uniformes » du §4.1 (prop. 4.5 et 4.6 et cor. 4.7 et 4.8) ne s'appliquent. Pour cette courbe, on a donc recours au critère du th. 4.1. Soit $p \geq 5$ un nombre premier exceptionnel. D'après le programme `TraceOfFrobenius`, on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|5} = \{-2, 1\} \quad \text{et} \quad t_7 = 6.$$

D'après le th. 4.1 appliquée à $\ell = 5$ et $\ell = 7$, p divise chacun des entiers $B_5^{(2)}$ et $B_7^{(2)}$. Or, d'après le programme `ExceptionalPrimes`, on a

$$B_5^{(2)} = 2^{28} \cdot 3^{16} \cdot 5^{39} \cdot 11^2 \cdot 17 \cdot 61 \cdot 73 \cdot 277 \cdot 397 \cdot 557 \cdot 653 \cdot 757 \cdot 23833$$

et

$$B_7^{(2)} = 2^{14} \cdot 3^8 \cdot 5^2 \cdot 7^{13} \cdot 11 \cdot 13^5 \cdot 37^2 \cdot 2089 \cdot 2689 \cdot 3889.$$

D'où

$$p \in \mathfrak{S}_5^{(2)} \cap \mathfrak{S}_7^{(2)} = \{2, 3, 5, 11\}.$$

Il ne reste donc plus qu'à traiter les cas $p = 2$, 3, 5 et 11. Or, E a bonne réduction en l'idéal premier $3\mathcal{O}_K$ et d'après le programme `TraceOfFrobenius`, on a

$$P_3(X) = X^2 + 3X + 9.$$

Donc P_3 est irréductible modulo 2, 5 et 11. Et, si $\mathfrak{p}_5$ est un idéal premier au-dessus de 5, on a $t_{\mathfrak{p}_5} = -2$ ou 1, et

$$P_{\mathfrak{p}_5}(X) \equiv X^2 + 2X + 2 \pmod 3.$$

Donc $P_{\mathfrak{p}_5}$ est irréductible modulo 3. On en déduit que ρ_p est également irréductible pour $p = 2$, 3, 5 et 11. D'où le résultat.

Exemple 4.33 *On suppose $K = \mathbf{Q}(\sqrt{-6})$. On considère la courbe E d'équation*

$$y^2 = x^3 - 2(5 + 6\sqrt{-6})x - 2^3 \cdot 3^5. \tag{4.19}$$

Alors, l'ensemble $\mathrm{Exc}(E)$ *est vide.*

Démonstration. On a

$$\begin{cases} c_4 &= 2^5 \cdot 3(5 + 6\sqrt{-6}) \\ c_6 &= 2^8 \cdot 3^8 \\ \Delta &= -2^9(3191761 + 846\sqrt{-6}) \end{cases}$$

et $N_{K/\mathbf{Q}}(3191761 + 846\sqrt{-6}) = 7 \cdot 249947 \cdot 5822573$. La courbe E a mauvaise réduction multiplicative en un idéal au-dessus de 7, 249947 et 5822573. Par ailleurs, 2 est ramifié dans K. Posons $2\mathcal{O}_K = \mathfrak{p}_2^2$. En $\mathfrak{p}_2$, on a

$$(v_{\mathfrak{p}_2}(c_4), v_{\mathfrak{p}_2}(c_6), v_{\mathfrak{p}_2}(\Delta)) = (10, 16, 18).$$

Donc E a mauvaise réduction additive en $\mathfrak{p}_2$ avec potentiellement bonne réduction. De plus, on a $v_{\mathfrak{p}_2}(j) = 12$ et $2v_{\mathfrak{p}_2}(c_6) = 3v_{\mathfrak{p}_2}(c_4) + 2$. Posons $\pi = \sqrt{-6}$. C'est une uniformisante de $K_{\mathfrak{p}_2}$ et on a

$$\frac{c_4}{\pi^{10}} = -\frac{5 + 6\pi}{3^4} \equiv 1 + \pi^2 + \pi^3 \pmod{4\mathbf{Z}_2[\sqrt{-6}]}.$$

Donc, d'après [Bil08b, th.2], ni la condition (C1'), ni la condition (C3) n'est satisfaite et $|\Phi_{\mathfrak{p}_2}| = 4$.

Vu l'étude précédente, aucun des résultats « uniformes » du §4.1 (prop. 4.5 et 4.6 et cor. 4.7 et 4.8) ne s'appliquent. Pour cette courbe, on a donc recours au critère du th. 4.1. Les premiers ramifiés dans K sont 2 et 3. Soit $p \geq 5$ un nombre premier exceptionnel. D'après le programme `TraceOfFrobenius`, on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|11} = \{-4, 3\} \quad \text{et} \quad t_{13} = -8.$$

Donc d'après le théorème 4.1 appliqué à $\ell = 11$ et $\ell = 13$ et le programme `ExceptionalPrimes`, on a

$$p \in \mathfrak{S}_{11}^{(2)} \cap \mathfrak{S}_{13}^{(2)} = \{2, 5, 7\}.$$

Il ne reste donc plus qu'à traiter les cas $p = 2$, 3, 5 et 7 (car 3 est ramifié dans K). D'après le programme `TraceOfFrobenius`, on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|5} = \{-3, -2\} \quad \text{et} \quad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|11} = \{-4, 3\}.$$

On désigne par $\mathfrak{p}_5$ (resp. $\overline{\mathfrak{p}_5}$) l'idéal premier au-dessus de 5 tel que $t_{\mathfrak{p}_5} = -3$ (resp. $t_{\overline{\mathfrak{p}_5}} = -2$). Alors,

$$P_{\mathfrak{p}_5}(X) = X^2 + 3X + 5$$

est irréductible modulo 2 et 7. Par ailleurs, le polynôme

$$P_{\overline{\mathfrak{p}_5}}(X) = X^2 + 2X + 5$$

est irréductible modulo 3. De même, on désigne par $\mathfrak{p}_{11}$ l'idéal premier au-dessus de 11 tel que $t_{\mathfrak{p}_{11}} = -4$. Alors,

$$P_{\mathfrak{p}_{11}}(X) = X^2 + 4X + 11$$

est irréductible modulo 5. D'où le résultat.

Exemple 4.34 *On suppose* $K = \mathbf{Q}(\sqrt{2})$ *et on pose*

$$\begin{cases} A &= -3^3 \cdot 5 \cdot 17^3(428525 + 303032\sqrt{2}) \\ B &= 2 \cdot 3^3 \cdot 5 \cdot 17^3(62176502533 + 43965551956\sqrt{2}). \end{cases}$$

On considère la courbe E *d'équation*

$$y^2 = x^3 + Ax + B.$$

Alors, $\mathrm{Exc}(E) = \{13\}$.

Démonstration. On vérifie que pour le modèle choisi, on a

$$N_{K/\mathbf{Q}}(\Delta) = -2^{25} \cdot 3^{18} \cdot 5^4 \cdot 7^2 \cdot 17^{15} \cdot 23^6 \cdot 79^6.$$

En particulier, la courbe E a bonne réduction en les idéaux premiers divisant 11, 13, 19, 29 et 41 et d'après le programme `TraceOfFrobenius`, on a

$$t_{11} = 4; \quad t_{13} = -14 \quad t_{19} = 26; \quad t_{29} = 1 \quad \text{et} \quad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|41} = \{-3, 2\}.$$

Soit p un nombre premier exceptionnel n'appartenant pas à l'ensemble

$$\{2, 3, 5, 7, 17, 23, 79\}.$$

Alors, d'après le corollaire 4.2, on a en particulier

$$p \in \mathfrak{S}_{11}^{(2)} \cap \mathfrak{S}_{13}^{(2)}.$$

D'où, d'après le programme `ExceptionalPrimes`,

$$p \in \{2, 3, 5, 7, 13\}.$$

Autrement dit, il ne reste plus qu'à traiter les cas où $p = 2, 3, 5, 7, 13, 17, 23$ et 79. Or le polynôme P_{11} est irréductible modulo 5, 23 et 79. De même, P_{13} est irréductible modulo 7, P_{19} modulo 17 et P_{29} modulo 2. Si $\mathfrak{p}_{41}$ désigne l'idéal premier de $\mathcal{O}_K$ au-dessus de 41 tel que $t_{\mathfrak{p}_{41}} = 2$, alors $P_{\mathfrak{p}_{41}}$ est irréductible modulo 3. On en déduit que $2, 3, 5, 7, 17, 23$ et 79 ne sont pas exceptionnels. En revanche 13 est un nombre premier exceptionnel. En effet, la courbe modulaire $X_0(13)$ paramétrisant les courbes elliptiques munies d'un sous-groupe stable d'ordre 13 est de genre 0 et un isomorphisme avec $\mathbf{P}^1$ est donné par la fraction rationnelle suivante ([Mes80, §2.2]) :

$$j(X_0(13))(X) = \frac{(X^2 + 5X + 13)(X^4 + 7X^3 + 20X^2 + 19X + 1)^3}{X}.$$

On vérifie alors que l'on a $j(X_0(13))(\sqrt{2}) = j$. Cela montre que 13 est exceptionnel et le résultat annoncé.

Exemple 4.35 *On suppose* $K = \mathbf{Q}(\sqrt{3})$ *et on pose*

$$\begin{cases} a_1 &= 2^2 \cdot 7\sqrt{3}(1+2\sqrt{3})(2-\sqrt{3}) = 252 - 112\sqrt{3} \\ a_4 &= 2 \cdot 3^2 \cdot 7^2\sqrt{3}(1+2\sqrt{3})^2 = 10584 + 11466\sqrt{3} \\ a_6 &= 2^3 \cdot 3 \cdot 7^4\sqrt{3}(1+2\sqrt{3})^4(7-4\sqrt{3}) = -24202080 + 15616104\sqrt{3}. \end{cases}$$

On considère la courbe E *d'équation*

$$y^2 + a_1xy = x^3 + a_4x + a_6. \tag{4.20}$$

Alors, la courbe E *a des multiplications complexes par le corps* $\mathbf{Q}(\sqrt{-1})$ *et* $\mathrm{Exc}(E) = \{2, 3\}$.

Démonstration. On a

$$\begin{cases} c_4 &= -2^5 \cdot 3^2 \cdot 7^2 \cdot 11^2(-1+2\sqrt{3})(2-3\sqrt{3})^3\varepsilon^{-2} \\ c_6 &= 2^9 \cdot 3^3 \cdot 7^4 \cdot 11^3(1+2\sqrt{3})(2-3\sqrt{3})^3\varepsilon^{-4} \\ \Delta &= -2^9 \cdot 3^4 \cdot 7^6 \cdot 11^6\sqrt{3}(2-3\sqrt{3})^6\varepsilon^{-4} \end{cases}$$

où $\varepsilon = 2 + \sqrt{3}$ est l'unité fondamentale de $\mathbf{Q}(\sqrt{3})$. On en déduit que

$$\begin{aligned} j &= 2^6 \cdot 3 \cdot \sqrt{3}(-1+2\sqrt{3})^3(2-3\sqrt{3})^3\varepsilon^{-2} \\ &= 76771008 - 44330496\sqrt{3} \end{aligned}$$

est entier de polynôme minimal sur $\mathbf{Q}$

$$P(X) = X^2 - 153542016X - 1790957481984.$$

Vérifions que E a des multiplications complexes par l'ordre de $\mathbf{Q}(\sqrt{-1})$ de conduteur 3. En effet, il n'y a qu'un nombre fini de classes d'isomorphisme de courbes elliptiques ayant des multiplications complexes par un ordre de discriminant D fixé. De plus, le polynôme minimal sur $\mathbf{Q}$ de l'invariant modulaire d'une telle courbe elliptique est

$$\Phi_D(X) = \prod_{a,b,c} \left(X - j\left(\frac{-b+\sqrt{D}}{2a} \right) \right),$$

où j désigne la fonction modulaire et (a, b, c) parcourt l'ensemble des triplets d'entiers tels que la forme quadratique $ax^2 + bxy + cy^2$ soit primitive positive réduite de discriminant D ([Coh93, Th. 7.2.14]). Dans le cas où $D = -36$, on a exactement deux représentants des classes d'équivalence de telles formes quadratiques donnés par

$$x^2 + 9y^2 \quad \text{et} \quad 2x^2 + 2xy + 5y^2.$$

On vérifie alors que l'on a

$$\begin{aligned} \Phi_{-36}(X) &= (X - j(3\sqrt{-1}))\left(X - j\left(\frac{-1+3\sqrt{-1}}{2} \right) \right) \\ &= X^2 - 153542016X - 1790957481984 = P(X) \end{aligned}$$

et

$$j = j\left(\frac{-1+3\sqrt{-1}}{2}\right).$$

Cela établit l'assertion.

Par ailleurs, d'après l'expression des coefficients c_4, c_6 et Δ ci-dessus, E a réduction additive en l'idéal $\mathfrak{p}_3 = \sqrt{3}\mathcal{O}_K$ et

$$(v_{\mathfrak{p}_3}(c_4), v_{\mathfrak{p}_3}(c_6), v_{\mathfrak{p}_3}(\Delta)) = (4, 6, 9).$$

En particulier, on a d'après [Kra90, th. 1], $|\Phi_{\mathfrak{p}_3}| = 4$ ou 12. Donc, d'après le cor. 4.8, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$. Par ailleurs, la courbe modulaire $X_0(3)$ paramétrisant les courbes elliptiques munies d'un sous-groupe stable d'ordre 3 est de genre 0 et un isomorphisme avec $\mathbf{P}^1$ est donné par la fraction rationnelle suivante :

$$j(X_0(3))(X) = \frac{(X+3)^3(X+27)}{X}.$$

On vérifie alors que l'on a $j(X_0(3))(243 - 162\sqrt{3}) = j$. Cela montre que 3 est exceptionnel. On vérifie enfin que le point de coordonnées affines

$$\begin{cases} x &= -2^2 \cdot 7(15 + 8\sqrt{3}) \\ y &= 2^3 \cdot 3 \cdot 7^2(13 + 4\sqrt{3}) \end{cases}$$

est un point d'ordre 2 de E. En particulier, 2 est exceptionnel. D'où le résultat.

Remarques.

1. Pour montrer la finitude de l'ensemble exceptionnel, on aurait pu appliquer directement le cor. 4.2 (au lieu du cor. 4.8) par exemple avec le nombre premier $\ell = 5$ pour lequel $B_5^{(2)} \neq 0$.
2. Étant donné un entier $d \geq 1$, il existe un nombre fini de classes de $\overline{\mathbf{Q}}$-isomorphismes de courbes elliptiques à multiplications complexes définies sur un corps de nombres de degré $\leq d$. Pour un entier « raisonnable » d donné, il est de plus possible de calculer explicitement la liste des invariants modulaires des courbes à multiplications complexes définies sur un corps de degré $\leq d$. Nous avons entrepris de le faire dans le cas où $d = 2$ mais par manque de temps nous n'avons pas fini ces calculs. L'invariant modulaire j de la courbe d'équation (4.20) ci-dessus fait partie de cette liste.

Exemple 4.36 *On suppose $K = \mathbf{Q}(\sqrt{-3})$. On considère la courbe E définie sur K par l'équation*

$$y^2 = x^3 + 1.$$

Alors, E a mauvaise réduction additive en l'idéal premier $2\mathcal{O}_K$ avec un défaut de semi-stabilité d'ordre 3 et

$$\mathrm{Exc}(E) = \{2, 3\} \cup \{p \text{ premier } \mid p \equiv 1 \pmod 3\}.$$

Démonstration. Il s'agit de la courbe d'invariant modulaire nul notée 36A1 dans les tables de Cremona [Cre97]. Sur $\mathbf{Q}$ elle a réduction additive en 2 et son défaut de semi-stabilité est d'ordre 3 ([Kra90, cor. p.357]). Il en va même sur K car 2 est

non ramifié dans K. Le point de coordonnées $(-1,0)$ est d'ordre 2 et $(0,1)$ d'ordre 3. Soit p un nombre premier ≥ 5. Vu la théorie de la multiplication complexe, si $p \equiv 1 \pmod 3$, alors la représentation $\rho_p : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ a pour image le normalisateur d'un sous-groupe de Cartan déployé de $\mathrm{GL}_2(\mathbf{F}_p)$. Sa restriction à G_K a précisément pour image ce sous-groupe de Cartan déployé. En particulier, elle est réductible. En revanche, si $p \equiv 2 \pmod 3$, alors d'après [Ser72, p. 275], l'image par ρ_p de $\mathrm{G}_{\mathbf{Q}}$ est le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_p)$. La restriction de ρ_p à G_K a alors pour image ce sous-groupe de Cartan non déployé. En particulier, elle est irréductible. D'où le résultat.

4.6.4 Un exemple sur un corps cubique

Exemple 4.37 *On suppose $K = \mathbf{Q}(\alpha)$ où α est une racine dans $\overline{\mathbf{Q}}$ du polynôme $X^3 - 3X + 1$. On considère la courbe E d'équation*

$$y^2 = x^3 + 2(1+\alpha)^2 x + 24\alpha(2+\alpha).$$

Alors, l'ensemble $\mathrm{Exc}(E)$ *est vide.*

Démonstration. On a $D_K = 3^4$ et $3\mathcal{O}_K = \mathfrak{p}_3^3$ où $\mathfrak{p}_3$ est l'idéal de $\mathcal{O}_K$ engendré par $1+\alpha$. De plus, on vérifie que l'on a

$$\begin{cases} c_4 &= -2^5(1+\alpha)^5(1+\alpha-\alpha^2); \\ c_6 &= -2^8(1+\alpha)^{12}(1+\alpha-\alpha^2)^3; \\ \Delta &= -2^9(1+\alpha)^6 \cdot 5 \cdot 11 \end{cases}$$

et $1+\alpha-\alpha^2$ est une unité de $\mathcal{O}_K$. La courbe E a mauvaise réduction multiplicative en les idéaux premiers $5\mathcal{O}_K$ et $11\mathcal{O}_K$. En l'idéal premier $\mathfrak{p}_3$, la courbe a mauvaise réduction additive avec potentiellement bonne réduction et $v_{\mathfrak{p}_3}(\Delta_{\mathfrak{p}_3}) = v_{\mathfrak{p}_3}(\Delta) = 6$. Donc, d'après [Kra90, th.1], on a $|\Phi_{\mathfrak{p}_3}| = 2$ ou 6. En l'idéal premier $2\mathcal{O}_K$, la courbe E a mauvaise réduction additive avec potentiellement bonne réduction et

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (5, 8, 9)$$

d'où $v_2(j) = 6$ et $2v_2(c_6) = 3v_2(c_4) + 1$. Comme de plus

$$j' = \frac{j}{2^6} = \frac{(1+\alpha)^9(1+\alpha-\alpha^2)^3}{5 \cdot 11} = \frac{3^3}{5 \cdot 11} \equiv 1 \pmod 4,$$

d'après [Cal04], on a $|\Phi_2| = 4$. Partout ailleurs, la courbe E a bonne réduction.

Vu l'étude précédente, aucun des résultats « uniformes » du §4.1 ne s'appliquent. Les nombres premiers 17, 19, 37 et 53 sont (totalement) décomposés dans K et on vérifie que l'on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|17} = \{-3,-3,3\}; \qquad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|19} = \{-5,-5,5\};$$
$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|37} = \{-7,-7,7\}; \qquad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|53} = \{-3,3,3\}.$$

Soit p un nombre premier exceptionnel ≥ 5. D'après le th. 4.1, on a en particulier,

$$p \in \mathfrak{S}_{17}^{(3)} \cap \mathfrak{S}_{19}^{(3)} \cap \mathfrak{S}_{37}^{(3)} = \{2,3,5\}.$$

Il ne reste donc plus qu'à traiter les cas où $p = 2, 3$ ou 5. Or, si $\mathfrak{p}_{53}$ désigne un idéal premier de $\mathcal{O}_K$ au-dessus de 53, le polynôme $P_{\mathfrak{p}_{53}}$ est irréductible modulo 2 et 5. Par ailleurs, l'idéal $7\mathcal{O}_K$ est premier et $t_7 = -36$, donc le polynôme

$$P_7(X) = X^2 + 36X + 7^3$$

est irréductible modulo 3. On en déduit le résultat annoncé.

Bibliographie

[AL70] A. O. L. Atkin et J. Lehner. Hecke Operators on $\Gamma_0(m)$. *Math. Ann.*, 185 :134–160, 1970.

[BB02] M. Bauer et M. Bennett. Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. *Ramanujan J.*, 6(2) :209–270, 2002.

[BVY04] M. A. Bennett, V. Vatsal, et S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6) :1399–1416, 2004.

[Beu81] F. Beukers. On the generalized Ramanujan-Nagell equation. I. *Acta Arith.*, 38(4) :389–410, 1980/81.

[Bil07] N. Billerey. Équations de Fermat de type $(5, 5, p)$. *Bull. Austral. Math. Soc.*, 76(2) :161–194, 2007.

[Bil08a] _____ Formes homogènes de degré 3 et puissances p-ièmes. *J. Number Theory*, 128(5) :1272–1294, 2008.

[Bil08b] _____. Sur le défaut de semi-stabilité des courbes elliptiques. 2008. Soumis.

[BD08] N. Billerey et L. V. Dieulefait. Solving Fermat-type equations $x^5 + y^5 = dz^p$. *arXiv :0802.1217v2*, 2008. A paraître dans Math. Comp.

[Bou81] N. Bourbaki. *Éléments de mathématique*, volume 864 of *Lecture Notes in Mathematics*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, et R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercices. *J. Amer. Math. Soc.*, 14 :843–939, 2001.

[BHM02] Y. Bugeaud, G. Hanrot, et M. Mignotte. Sur l'équation diophantienne $(x^n - 1)/(x - 1) = y^q$. III. *Proc. London Math. Soc. (3)*, 84(1) :59–78, 2002.

[Cal04] É. Cali. Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié. *Canad. J. Math.*, 56(4) :673–698, 2004.

[CK02] É. Cali et A. Kraus. Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, $\ell \neq p$. *Acta Arith.*, 104 :1–21, 2002.

[CS09] I. Chen et S. Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322 :638–656, 2009.

[Coh93] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh00] _____. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Cre97] J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Dar93] H. Darmon. The equation $x^4 - y^4 = z^p$. *C. R. Math. Rep. Acad. Sci. Canada*, 15(6) :286–290, 1993.

[Dar95] _____. The Shimura-Taniyama conjecture (after Wiles). *Uspekhi Mat. Nauk*, 50(3(303)) :33–82, 1995.

[Dar97] _____. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1) :3–14, 1997.

[DG95] H. Darmon et A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27 :513–544, 1995.

[Dav08] A. David. Caractère d'isogénie et borne uniforme pour les homothéties. *Thèse de l'université de Strasbourg*, 2008.

[Del85] P. Deligne. Représentations l-adiques. *Astérisque*, (127) :249–255, 1985. Seminar on arithmetic bundles : the Mordell conjecture (Paris, 1983/84).

[Dia95] F. Diamond. The refined conjecture of Serre. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 22–37. Int. Press, Cambridge, MA, 1995.

[Die05a] L. V. Dieulefait. Modular congruences, **Q**-curves and the Diophantine equation $x^4 + y^4 = z^p$. *Bull. Belg. Math. Soc. Simon Stevin*, 12(3) :363–369, 2005.

[Die05b] _____. Solving Diophantine equations $x^4 + y^4 = qz^p$. *Acta Arith.*, 117(3) :207–211, 2005.

[Dir28] L. Dirichlet. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. *J. reine angew. Math.*, 3 :354–375, 1828.

[Ell04] J. Ellenberg. Galois representations attached to **Q**-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126, 2004.

[Fal86] G. Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986.

[Fre86] G. Frey. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1 :1–40, 1986.

[GT02] A. Granville et T. Tucker. It's as easy as *abc*. *Notices Amer. Math. Soc.*, 49(10) :1224–1231, 2002.

[HK02] E. Halberstadt et A. Kraus. Courbes de Fermat : résultats et problèmes. *J. reine angew. Math.*, 548 :167–234, 2002.

[Hin08] M. Hindry. *Arithmétique*. Tableau Noir. Calvage & Mounet, 2008.

[HS00] M. Hindry et J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Ivo04] W. Ivorra. Courbes elliptiques sur **Q**, ayant un point d'ordre 2 rationnel sur **Q**, de conducteur $2^N p$. *Dissert. Math.*, 429, 2004.

[Ken82] M. A. Kenku. On the Number of **Q**-isomorphism Classes of Elliptic Curves in Each **Q**-Isogeny Class. *J. Number Theory*, 15(2) :199–202, 1982.

[Kra89] A. Kraus. Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.*, 54 :75–80, 1989.

[Kra90] _____. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4) :353–385, 1990.

[Kra95] _____. Une remarque sur les points de torsion des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 321(9) :1143–1146, 1995.

[Kra96] _____. Courbes elliptiques semi-stables et corps quadratiques. *J. Number Theory*, 60 :245–253, 1996.

[Kra97a] _____. Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique. *Dissertationes Math.*, 364, 1997.

[Kra97b] _____. Majorations effectives pour l'équation de Fermat généralisée. *Can. J. Math.*, 49(6) :1139–1161, 1997.

[Kra98] _____. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1) :1–13, 1998.

[Kra99] _____. On the equation $x^p + y^q = z^r$: A Survey. *The Ramanujan Journal*, 3(3) :315–333, 1999.

[Kra02] _____. Une question sur les équations $x^m - y^m = Rz^n$. *Compositio Math.*, 132 :1–26, 2002.

[Kra07] _____. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4) :611–633, 2007.

[KO92] A. Kraus et J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293 :259–275, 1992.

[Lan99a] M. Langevin. Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (*abc*). *J. Théor. Nombres Bordeaux*, 11(1) :91–109, 1999. Les XXèmes Journées Arithmétiques (Limoges, 1997).

[Lan99b] _____. Liens entre le théorème de Mason et la conjecture (*abc*). In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 187–213. Amer. Math. Soc., Providence, RI, 1999.

[Lig75] G. Ligozat. *Courbes modulaires de genre* 1. Société Mathématique de France, 1975. Bull. Soc. Math. France, Mém. 43.

[MW93] D. W. Masser et G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3) :247–254, 1993.

[Maz78] B. Mazur. Rational Isogenies of Prime Degree. *Invent. Math.*, 44, 1978.

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3) :437–449, 1996.

[Mes80] J.-F. Mestre. Points rationnels de la courbe modulaire $X_0(169)$. *Ann. Inst. Fourier (Grenoble)*, 30(2) :v, 17–27, 1980.

[Mom95] F. Momose. Isogenies of prime degree over number fields. *Compositio Math.*, 97(3) :329–348, 1995.

[Nag02] T. Nagell. *Collected papers of Trygve Nagell. Vol. 1*, volume 121 of *Queen's Papers in Pure and Applied Mathematics*. Queen's University, Kingston, ON, 2002. Edité par Paulo Ribenboim.

[Neu86] J. Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1986.

[Oes88] J. Oesterlé. Nouvelles approches du "théorème" de Fermat. *Sém. Bourbaki*, (694) :165–186, 1987-88.

[Pap93] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2) :119–152, 1993.

[Pel01] F. Pellarin. Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques. *Acta Arith.*, 100(3) :203–243, 2001.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100 :431–476, 1990.

[Rib94] ———. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[Ser68] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. McGill University. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser72] ———. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15 :259–331, 1972.

[Ser79] ———. Points rationnels des courbes modulaires $X_0(N)$ [d'après Barry Mazur]. In *Séminaire Bourbaki, 30e année (1977/78)*, volume 710 of *Lecture Notes in Math.*, pages Exp. No. 511, pp. 89–100. Springer, Berlin, 1979.

[Ser87] ———. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54 :179–230, 1987.

[Ser96] ———. Travaux de Wiles (et Taylor, ...). I. *Astérisque*, (237) :Exp. No. 803, 5, 319–332, 1996. Séminaire Bourbaki, Vol. 1994/95.

[Ser97] ———. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown.

[ST68] J.-P. Serre et J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88 :492–517, 1968.

[Sil92] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1992.

[Spr93] V. Sprindžuk. *Classical Diophantine equations*, volume 1559 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1993. Translated from the 1982 Russian original.

[Ste06] W. Stein. The Modular Forms Database. `http ://modular.fas.harvard.edu/Tables`, 2006.

[Szp90] L. Szpiro. Discriminant et conducteur des courbes elliptiques. *Astérisque*, (183) :7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. in *Modular functions of one variable, Lect. Notes in Math.*, 273 :33–52, 1975.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.*, 141(3) :443–551, 1995.

Résumé

Cette thèse est composée de deux parties indépendantes. Dans la première, on s'intéresse à la résolution de certaines équations diophantiennes par la méthode modulaire. On traite plus particulièrement le cas des équations de Fermat de type $(5, 5, p)$ ainsi que celui des équations de la forme $F(x, y) = z^p$ où p est un nombre premier et F une cubique rationnelle.

La deuxième partie est consacrée à l'arithmétique des courbes elliptiques. Dans le cas d'une courbe définie sur une extension finie de $\mathbf{Q}_2$ ayant mauvaise réduction additive avec potentiellement bonne réduction, on s'intéresse à la détermination de son défaut de semi-stabilité. On énonce un résultat partiel valable pour toute extension finie de $\mathbf{Q}_2$. Dans le cas des extensions quadratiques ramifiées de $\mathbf{Q}_2$, on obtient un résultat complet. Par ailleurs, si E est une courbe elliptique définie sur un corps de nombres K, on s'intéresse, dans le dernier chapitre, à l'ensemble des nombres premiers p pour lesquels l'action du groupe de Galois absolu de K sur le sous-groupe des points de p-torsion de E est réductible. Lorsque cet ensemble est fini, on obtient un critère permettant en pratique de le déterminer explicitement.

Mots-clés :

Équations diophantiennes, courbes elliptiques, formes modulaires, représentations galoisiennes, théorie du corps de classes.

Abstract

This thesis has two independant parts. In the first one, we are interested in solving some diophantine equations using the modular method. We especially focus on Fermat equations of type $(5, 5, p)$ and equations of the shape $F(x, y) = z^p$ where p is prime number and F a rational cubic.

The second part deals with arithmetic of elliptic curves. We are interested in calculating the defect of semi-stability of an elliptic curve defined over a finite extension of $\mathbf{Q}_2$ and having additive bad reduction with potentially good reduction. We state a partial result valid for every finite extension of $\mathbf{Q}_2$. In the case of quadratic extensions, we get a complete result. Besides, let E be an elliptic curve defined over a number field K. In the last chapter, we look at prime numbers p such that the Galois action of K on the group of p-torsion points of E is reducible. In case this set is finite, we state a result which allows us in practice to determine it explicitely.

Keywords :

Diophantine equations, elliptic curves, modular forms, Galois representations, class field theory.